



ENGLISH TRANSLATION OF  
JAPANESE PATENT APPLICATION  
10-324169

## Specification

### 1. Title of the Invention:

Method and Apparatus for Controlling Digital Data

### 2. Claims:

- (1) A method of recording digital data onto a medium, comprising the steps of:
  - (a) detecting from digital data any additional information electronically embedded therein;
  - (b) if said additional information is detected, then performing access control for the digital data using said additional information;
  - (c) scrambling the digital data; and
  - (d) recording the scrambled digital data onto a medium.
- (2) The method of claim 1, wherein said step (b) comprises a step of determining whether copying/recording of the digital data is to be stopped or continued.
- (3) The method of claim 2, wherein said step (b) further comprises a step of embedding a copy mark into the digital data in accordance with a content of said additional information.
- (4) A method of performing playback control of digital data recorded onto a medium, comprising the steps of:
  - (a) descrambling scrambled digital data;
  - (b) detecting from the digital data any additional information and copy mark electronically embedded therein; and
  - (c) performing playback control of the digital data using said additional information and copy mark.

(5) The method of claim 1 or 4, wherein said electronically embedded additional information comprises such additional information that is embedded through a transformation of the data itself.

(6) A video driver card for creating digital data, comprising:

(a) an encoder for receiving analog data and outputting digital data;

(b) means for detecting any additional information electronically embedded in the digital data;

(c) means for adding a copy mark to said additional information in accordance with said additional information; and

(d) means for scrambling the digital data with said additional information.

(7) The video driver card of claim 6, wherein said digital data is an MPEG stream, and wherein said encoder is an MPEG encoder.

(8) A video driver card for decoding digital data, comprising:

(a) means for descrambling scrambled digital data;

(b) means for detecting from the digital data any additional information and copy mark electronically embedded therein; and

(c) means for performing playback control of the digital data using said additional information and copy mark.

(9) The video driver card of claim 8, wherein said digital data is an MPEG stream, and wherein said means (c) comprises means for determining whether or not outputting of an MPEG stream is to be performed and for outputting a desired MPEG stream.

(10) The video driver card of claim 6 or 8, wherein said electronically embedded additional information comprises such additional information that is embedded through a

transformation of the data itself.

(11) The video driver card of claim 9, wherein said means (c) further comprises means for adding a copy mark to the digital data in accordance with said additional information and copy mark and for outputting the digital data.

(12) A recorder for recording digital data onto a medium, comprising:

(a) an encoder for receiving analog data and outputting digital data;

(b) means for detecting any additional information electronically embedded in the digital data;

(c) means for adding a copy mark to said additional information in accordance with said additional information; and

(d) means for scrambling the digital data; and

(e) means for recording the scrambled digital data onto a medium.

(13) The recorder of claim 12, wherein said digital data is an MPEG stream, and wherein said encoder is an MPEG encoder.

(14) The recorder of claim 12, wherein said electronically embedded additional information comprises such additional information that is embedded through a transformation of the data itself.

(15) A player for playing back digital data recorded onto a medium, comprising:

(a) means for reading the digital data from the medium;

(b) means for descrambling the digital data;

(c) means for detecting from the digital data any additional information and copy mark electronically embedded therein; and

(d) means for performing playback control of the digital data

using said additional information and copy mark.

(16) The player of claim 15, wherein said digital data is an MPEG stream, and wherein said means (d) comprises means for determining whether or not outputting of an MPEG stream is to be performed and for outputting a desired MPEG stream.

(17) The player of claim 15, wherein said electronically embedded additional information comprises such additional information that is embedded through a transformation of the data itself.

(18) The player of claim 16, wherein said means (d) further comprises means for adding a copy mark to the digital data in accordance with said additional information and copy mark and for outputting the digital data.

### 3. Detailed Description of Invention:

[0001]

[Field of the Invention]

This invention relates to a technique for embedding additional information (digital watermark) into digital contents for copyright protection thereof, whereby a video recorder, a player or the like may detect such embedded additional information for use in control (management) of recording and playback of such digital contents. More specifically, this invention relates to a method and an apparatus, which use the digital watermarking and scrambling (or encrypting) techniques, for controlling recording and playback of such digital contents.

[0002]

## [Background Art]

As one of the methods of providing the safest and powerful control function for copyright protection of digital data, there is the access control method of data that uses the so-called digital watermarking. The digital watermarking is a technique for electronically embedding additional information into digital data (contents). Such additional information is embedded through a transformation of data itself. That is, digital data and additional information are unified or integrated together and, thus, it is difficult to separate the one from the other. In this respect, Japanese Patent Application 8-273551 discloses a prior technique for performing access control of data using this digital watermarking. More particularly, in Japanese Patent Application 8-273551, an additional information detector (digital watermark detector) is provided in a drive such as DVD for detecting such additional information from various MPEG streams and for performing access control using the same. Fig. 1 shows its schematic configuration. An STB (Set-Top Box) 110 supplies signals, which may be in analog or digital form, to a video recorder (recorder) 120. In case of feeding an MPEG stream from the STB 11, this MPEG stream is directly sent to the additional information detector in the video recorder 120. On the other hand, if an output of the STB 110 is in the analog form, this analog output is sent to an MPEG encoder in a video driver card for converting it into a digital signal, which is then sent to the additional information detector. This additional information detector detects any additional information and copy mark information embedded in the contents and, in accordance with the information, performs a variety of predetermined control with respect to the video

recorder 120 and a playback machine (player) 130. By way of example, the following items of control are performed.

[0003]

In a recording device, detection of a digital watermark is performed and, based on this, the following copying control operations are performed (Note that a symbol "CM" below stands for a copy mark).

(1,0) and absence of CM: Add a CM and passes the stream (authorize or permit video recording).

(1,0) and presence of CM: Stop the stream or video recording.

(1,1) : Stop the stream or video recording.

(0,0) or absence of detected additional information: Permit video recording.

[0004]

In a playback device, detection of a digital watermark is performed and, based on this, the following playback control operations are performed.

(1,0) and absence of CM: Prohibit playback.

(1,0) and presence of CM: Prohibit playback for a read-only disk, whereas permit playback for a write-once disk or a writable disk.

(1,1) : Permit playback for a read-only disk, whereas prohibit playback for a write-once disk or a writable disk.

(0,0) or absence of detected additional information: Permit playback.

[0005]

As described, Japanese Patent Application 8-273551 provides

some copying control techniques, as well as playback control techniques adapted for respective types of media. However, in accordance with this prior approach, it is necessary to provide the additional information detector in a drive (i.e., in a recording device or a playback device). This is because, in order to secure copyright protection, it is mandatory to provide the additional information detector at the reading nucleus of the video recorder 120, even though the video recorder 120 has severe constraints on its cost and/or space. Also, it is necessary to detect a digital watermark from a variety of MPEG streams, which should inevitably leads to upsizing of the detector. Further, in order to know in the playback machine 130 that the current contents are copied one, it is necessary to know information about types of the media (e.g., read-only, write-once and writable) that are subject to reading. Accordingly, what is needed is a new copyright protection scheme using digital watermarking, which is free of aforesaid problems.

[0006]

[Problems to be Solved by the Invention]

It is, therefore, an object of this invention to provide a method of controlling data copying or playback and an apparatus therefor, which do not require to provide an additional information detector in a drive that has severe constraints on its cost and/or space.

It is another object of this invention to provide a method of controlling data copying or playback and an apparatus therefor, which use an additional information detector of a smaller size. It is yet another object of this invention to provide a method of controlling data copying or playback and an apparatus therefor, which do not require to know information about types



of the media for playback control.

It is yet another object of this invention to provide a method of controlling data copying or playback and a system therefor, which use effectively combined digital watermarking and scrambling techniques.

[0007]

[Means for Solving the Problems]

To accomplish said objects, the recording control is performed as set forth below. First, from digital data, any additional information electronically embedded therein is detected and, if such additional information is detected, then access control of the digital data is performed using the additional information. Next, the digital data is scrambled for recording the same onto a medium. Note that the term "electronically embedded additional information" means herein such additional information that is embedded through a transformation of the data itself. Also, the term "access control" means herein to determine whether copying/recording of the digital data is to be stopped or continued. Depending on a content of the additional information, the term "access control" also embraces to embed control information such as a copy mark into the digital data.

Next, in case of playback control, the scrambled digital data is descrambled (or decrypted), thereby to detect any electronically embedded additional information and copy mark from the descrambled digital data. Using such detected information, playback control of the digital data is performed.

[0008]

Fig. 6 shows an exemplary flow chart for recording/copying

control. At step 610, digital data such as an MPEG stream is inputted, and at step 620, detection of any electronically embedded additional information is performed. At step 630, it is determined whether or not the additional information is detected, and if not, the stream is passed as it is. If the determination at step 630 is "YES", then at step 640, it is determined whether or not the additional information is (1,1), and if so, the stream is not passed. At the same time, scrambling or video recording is stopped. If the additional information is not (1,1), then at step 650, it is determined whether or not the additional information is (1,0). If this result is "YES", the stream is passed as it is. If the result of step 650 is "NO", then at step 660, it is determined whether or not the additional information is (0,0). If this result is "YES", then the stream is passed as it is. Otherwise, this means that the additional information is (0,1), which cannot possibly exist in any event and, thus, the additional information is determined to be undefined. Instead of doing this, however, the stream may be prohibited on an assumption that such abnormality has been caused by an erroneous bit change in the medium or another abnormality that occurred during embedding. The passed stream is subsequently scrambled for recording the same onto a medium. While said scrambling is a means for enciphering, it may be such scrambling based on an encryption key for improving robustness. Using such scrambling by an encryption key, there is no way to decode the scrambled digital data in the absence of the key and, thus, it becomes possible to distribute the digital contents in a safer manner.

[0009]

Fig. 7 shows an exemplary flow chart for playback control. At step 710, digital data is inputted, and at step 720, descrambling (decoding) of the scrambled digital data is

performed. At step 730, it is determined whether or not the decoding is terminated, and if so, the process proceeds to step 740. If the result at step 730 is "NO", then at step 760, it is determined whether or not another encryption technique such as CSS (Content Scramble System) has been applied. Note here that CSS is a scrambling technique for a read-only disk. If the result at step 760 is "YES", the corresponding decoding process is performed. Otherwise, the present playback is continued. After performing detection of the additional information at step 740, then at step 750, it is determined whether or not the detection is terminated. If this result is "NO", the process proceeds to step 760. On the other hand, if the result of step 750 is "YES", the process proceeds to step 765. At step 765, it is determined whether the detected additional information is (1,1) or (0,0) or absence of the additional information. If this result is "YES", the playback is continued. On the other hand, if this result is "NO", then at step 770, it is determined whether or not the additional information is (1,0). If this result is "NO", the additional information is deemed to be undefined. However, if this result is "YES", then the process proceeds to step 780. At step 780, it is determined whether or not there exists a copy mark, and if so, the playback is continued. On the other hand, if this result is "NO", then at step 790, a copy mark is added and the playback is continued. In this case, i.e., if the result of step 780 is "NO", the playback may be alternatively stopped.

[0010]

Incidentally, in a case where the digital data cannot be correctly descrambled (i.e., the digital data has not been scrambled), it may be alternatively processed as set forth below. For example, if the additional information is (1,0) and there is no copy mark, the stream is stopped and its descrambling or

playback is stopped. Also, if the additional information is (1,1) and there is a copy mark, the stream is stopped and its descrambling or playback is stopped. Further, if the additional information is (1,1), the stream, its descrambling and/or playback is stopped. Finally, if the additional information is (1,1) or there is no additional information at all, the playback is permitted.

[0011]

[Description of Embodiment of the Invention]

Now, with reference to the drawings, an embodiment of this invention will be described. Figs. 2 and 3 show schematic configurations of apparatuses of this invention for performing recording/playback of the digital data. While Fig. 2 shows an application of this invention to a video driver card primarily used in a personal computer in such a manner that a card is separated from a drive, Fig. 3 shows another application of this invention to a digital recorder (recorder) and a digital player (player) as representative electric home appliances in such a manner that a card and a drive are integrated together.

[0012]

In Fig. 2, there are two different signal flows involved. That is, in the first signal flow, a signal inputted into an STB 210 is fed from an analog output of the STB 210 to a video driver card of a recorder 220. Whereas in the second signal flow, detection of additional information, addition of a copy mark and scrambling are performed in the STB 210 and, then, the scrambled digital data is directly fed to a drive of the recorder 220. When an analog signal is inputted to the video driver card, it is converted to a digital data by an MPEG encoder such that

detection of additional information, addition of a copy mark and scrambling are subsequently performed. The digital data so scrambled is recorded onto a medium by the recorder 220. This medium is then conveyed to a player 230 for its playback. Note that the recorder 220 and player 230 are described herein to be separate machines, but they may be configured as a single machine. The latter approach would be more general than the former. The medium conveyed to the player 230 is subject to a reading operation. The digital data read from the medium is then inputted to a video driver card such that its descrambling, detection of the additional information and addition of a copy mark (if required) are subsequently performed. Finally, the digital data is decoded by an MPEG decoder.

[0013]

In Fig. 3, there are two different signal flows involved. That is, in the first signal flow, a signal inputted into an STB 310 is fed from an analog output of the STB 310 to a recorder 320. Whereas in the second signal flow, detection of additional information, addition of a copy mark and scrambling are performed in the STB 310 and, then, the scrambled digital data is directly fed to a drive of the recorder 320. When an analog signal is inputted to the recorder 320, it is converted to a digital data by an MPEG encoder such that detection of additional information, addition of a copy mark and scrambling are subsequently performed. The digital data so scrambled is recorded onto a medium by a recording device. This medium is then conveyed to a player 330 for its playback. Note that the recorder 320 and player 330 are described herein to be separate machines, but they may be configured as a single machine. The latter approach would be more general than the former. The medium conveyed to the player 330 is subject to a reading operation. The digital data read from the medium is then

inputted to a video driver card such that its descrambling, detection of the additional information and addition of a copy mark (if required) are subsequently performed. Finally, the digital data is decoded by an MPEG decoder.

[0014]

Fig. 8 is a block diagram, which shows a more detailed configuration of the recorder 320 or STB adapted for use in digital watermarking and scrambling. Block 810 is an input control circuit block for receiving an MPEG stream and passing the MPEG stream to a stream conversion circuit and an MPEG parser circuit. Block 820 is the MPEG parser circuit block for extracting from the MPEG stream those portions that are required by the next stage. Block 830 is a macro block buffer for storing at least one macro block that is necessary for embedding control information. Block 840 is a code amount comparison circuit block for calculating and comparing code lengths in a macro block. Block 850 is a code conversion circuit block for converting a code to be used for embedding the control information. Block 860 is a code amount adjustment circuit block for adjusting a code length to be identical to its value before the conversion and for forming the result as an embedding conversion table. Block 870 is a stream conversion circuit block for stopping/ converting/ passing the MPEG stream as it is based on a detected result of additional information. Block 880 is an accumulation memory for accumulating those values of DCT factors derived by the MPEG parser circuit that are multiplied by weighting factors. Block 890 is a table of the weighting factors for correlating with additional information contained in the inputted MPEG image. Block 892 is a statistical processing circuit block for performing statistical processing of the values stored in the accumulation memory. Block 897 is a detected result determination circuit block for determining

a value of embedded additional information from its preceding stage and for issuing an indication to the stream conversion circuit. Block 896 is a scramble circuit block for performing authentication with a recording device and for scrambling such stream that is found to contain the additional information.

[0015]

Fig. 9 is a block diagram, which shows a more detailed configuration of the player 330 adapted for use in descrambling and detection of the additional information. Block 910 is a descramble circuit block for authenticating an inputted digital signal with a playing device and for descrambling the digital signal. Block 920 is an input control circuit block for receiving the MPEG stream and passing the MPEG stream to a stream control circuit and an MPEG parser circuit. Block 930 is the MPEG parser circuit block for extracting from the MPEG stream those portions that are required by the next stage. Block 940 is an accumulation memory for accumulating those values of DCT factors derived by the MPEG parser circuit that are multiplied by weighting factors. Block 950 is a table of the weighting factors for correlating with additional information contained in the inputted MPEG image. Block 960 is a statistical processing circuit block for performing statistical processing of the values stored in the accumulation memory. Block 970 is a detected result determination circuit block for determining a value of embedded additional information from its preceding stage and for issuing an indication to the stream control circuit. Block 980 is the stream control circuit for stopping/passing the MPEG stream as it is based on the detected result of additional information.

[0016]

Fig. 4 shows paths of a signal, which is subject to prohibition of processing, and a medium in the prior scheme in case of only one generation copy is allowed. In a compliant device (a device in accordance with the prior scheme), a compliant source (a source in accordance with the prior scheme) 410 is smoothly processed in a recorder 420 and/or player 430, but no further recording can be performed in a recorder 440. Note, however, in this respect that in such an operation combined with a non-compliant device, it is possible to perform an illegal recording/playback operation. By way of example, if the compliant source 410 is digitally inputted to a recorder 450 in the non-compliant device, it is not only possible to perform its digital recording but also its playback in a player 460. Further, if a digital output of the player 430 in the compliant device is inputted to a recorder 470 in the non-compliant device, it becomes possible to perform its recording as well.

[0017]

Fig. 5 shows paths of a signal, which is subject to prohibition of processing, and a medium in accordance with the scheme of this invention. In a compliant device (a device in accordance with the scheme of this invention), a compliant source (a source in accordance with the scheme of this invention) 510 is smoothly processed in a recorder 520 and/or player 530, but no further recording can be performed in a recorder 540. Here, operations combined with a non-compliance device will be considered briefly. First, even if it is intended to digitally input the compliant source 510 to a recorder 550 in the non-compliant device, such inputting is prohibited and, thus, there will be no way to perform its digital recording. Also, it becomes possible to prohibit inputting of a digital output of the player 530 in the compliant device to a recorder 570 in the non-compliant device.



[0018]

Further, as another embodiment of playback control, for those scrambled contents of a read-only disk such as CSS, its playback may be permitted on a condition that CSS is successfully descrambled. More particularly, if CSS is successfully descrambled, it is possible to avoid detection of any digital watermark. Alternatively, if CSS is successfully descrambled, it is possible to permit playback on a condition that the additional information of (1,1) is detected. Further, by adding an scheme that allows to perform descrambling using proximately detected digital watermarking information and/or additional information as a key, or to perform subsequent descrambling using such digital watermarking information that is detected after the initial descrambling, it is possible to strengthen the protection function of scrambling and yet to cause detection of a digital watermark to be mandatory. In order to protect copying of scrambled digital data, by using such scrambling with an encryption key, it becomes possible to disable its playback even though its copying is done. Moreover, for those contents that are not subject to any copyright protection, it is also possible to avoid scrambling and/or embedding additional information therein, and to similarly apply descrambling in such a manner that any information to be displayed within a display unit such as a TV set is scrambled or additional information is detected, without departing the spirit of this invention.

[0019]

#### [Advantages of the Invention]

In accordance with this invention, there is provided a method

of controlling data copying or playback and an apparatus therefor, which use effectively combined digital watermarking and scrambling techniques. As a result, there is no need to provide an additional information detector in a drive that has severe constraints on its cost and/or space. Further, it becomes possible to prevent a compliant source from being digitally recorded and/or digitally played back at a recorder and/or a player in a non-compliant device respectively.

#### 4. Brief Description of the Drawings:

Fig. 1 is a diagram showing a prior scheme for performing access control of data.

Fig. 2 is a schematic diagram showing an apparatus of this invention for performing recording and playback of digital data.

Fig. 3 is another schematic diagram showing an apparatus of this invention for performing recording and playback of digital data.

Fig. 4 is a diagram showing paths of a signal, which is subject to prohibition of processing, and a medium in the prior scheme.

Fig. 5 is a diagram showing paths of a signal, which is subject to prohibition of processing, and a medium in accordance with the scheme of this invention.

Fig. 6 is an exemplary flow chart for recording/copying control.

Fig. 7 is an exemplary flow chart for playback control.

Fig. 8 is a block diagram showing a more detailed configuration of the apparatus for digital watermarking and scrambling.

Fig. 9 is a block diagram showing a more detailed configuration of the apparatus for descrambling and detection of additional information.

[Document type] Abstract

[Abstract]

[Object]

To provide a method of controlling data copying or playback and an apparatus therefor, which do not require to provide an additional information detector in a drive that has severe constraints on its cost and/or space.

[Constitution]

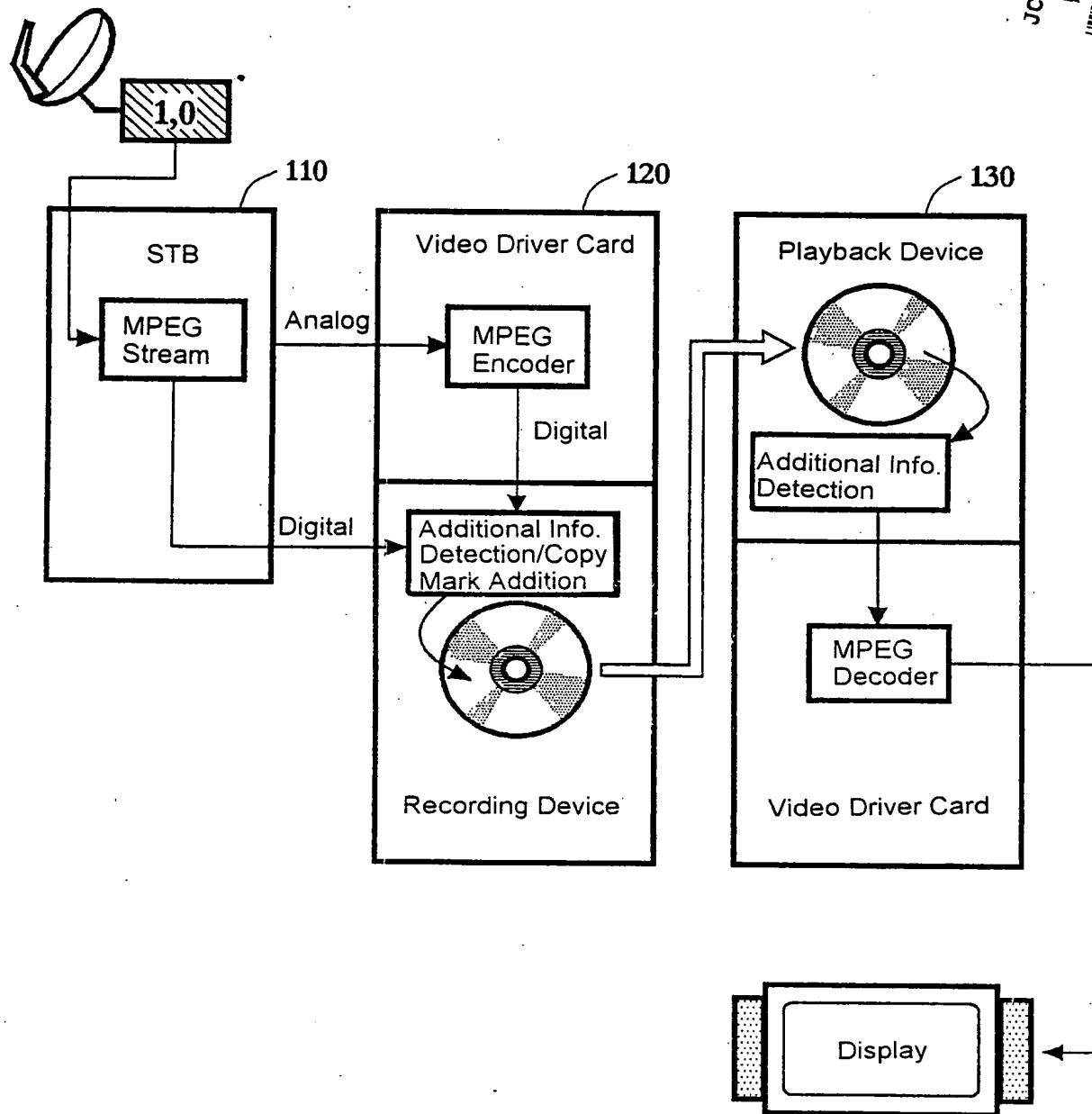
For the recording control, from digital data, any additional information electronically embedded therein is detected and, if such additional information is detected, then access control of the digital data is performed using the additional information. Next, the digital data is scrambled for recording the same onto a medium. Note that the term "electronically embedded additional information" means herein such additional information that is embedded through a transformation of the data itself. Also, the term "access control" means herein to determine whether copying/recording of the digital data is to be stopped or continued. Depending on a content of the additional information, the term "access control" also embraces to embed control information such as a copy mark into the digital data.

For the playback control, the scrambled digital data is descrambled, thereby to detect any electronically embedded additional information and copy mark from the descrambled digital data. Using such detected information, playback control of the digital data is performed.

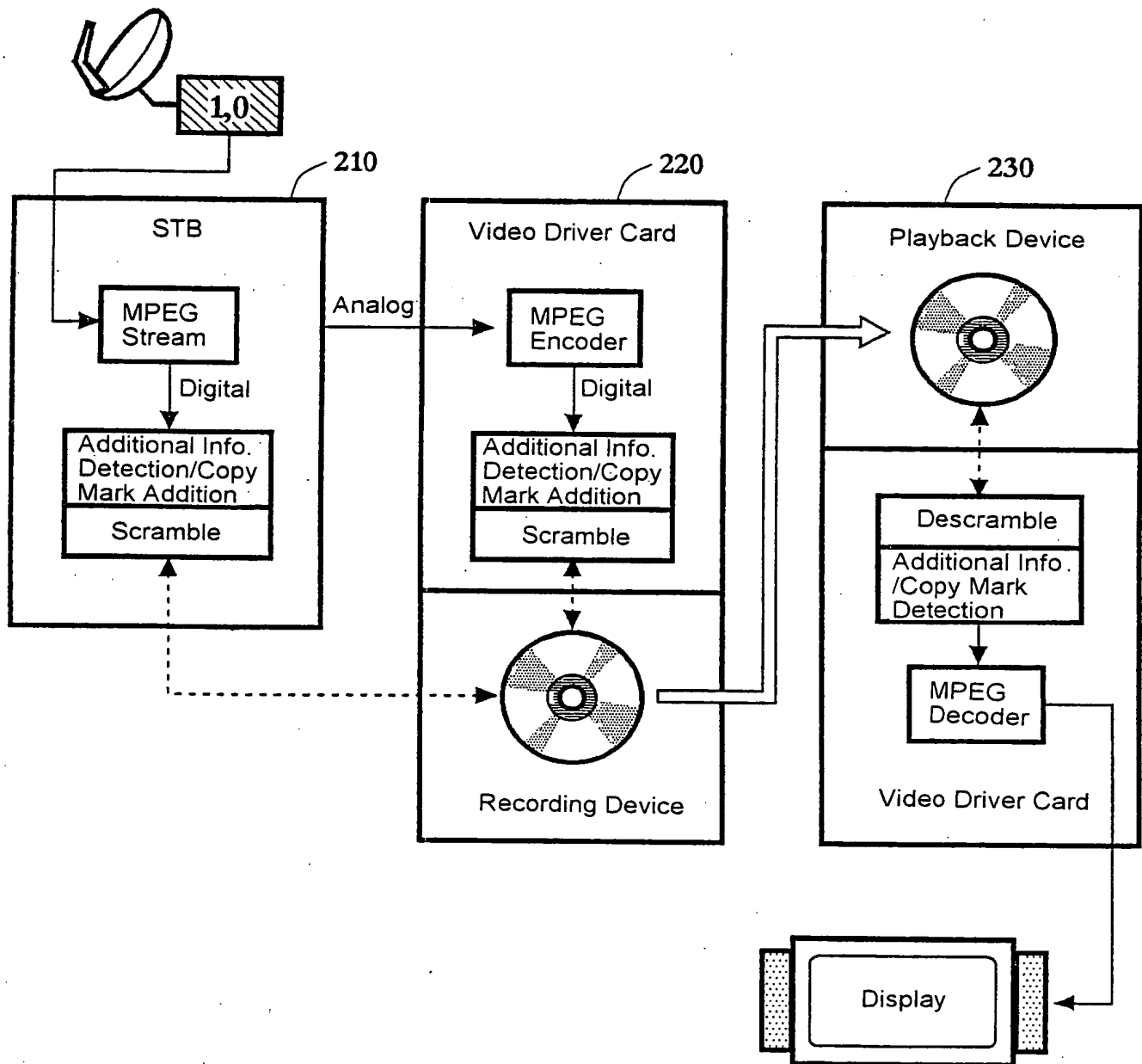
[Selected Drawing] Fig. 3

[Document Type] Drawing

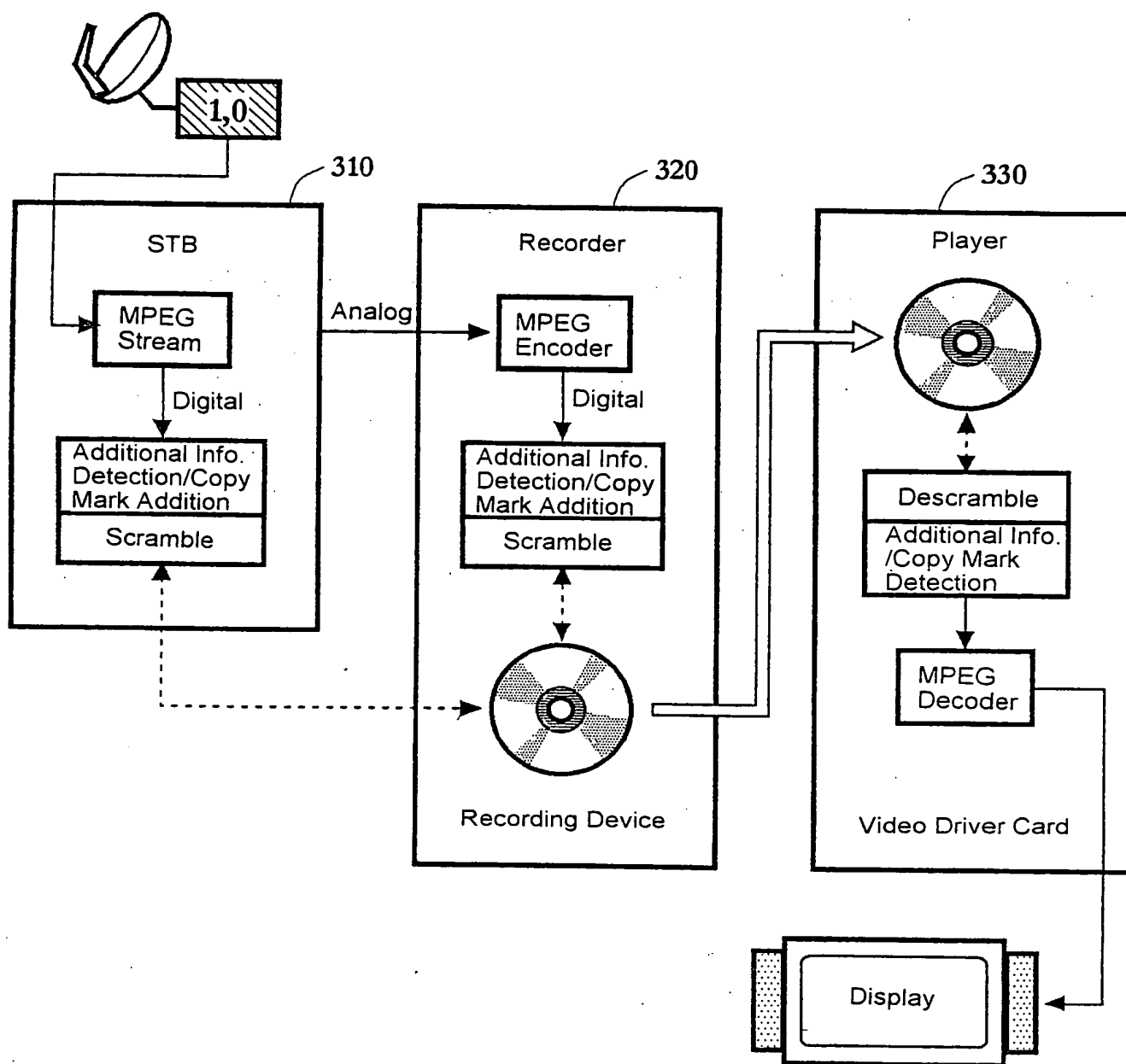
[Figure 1]



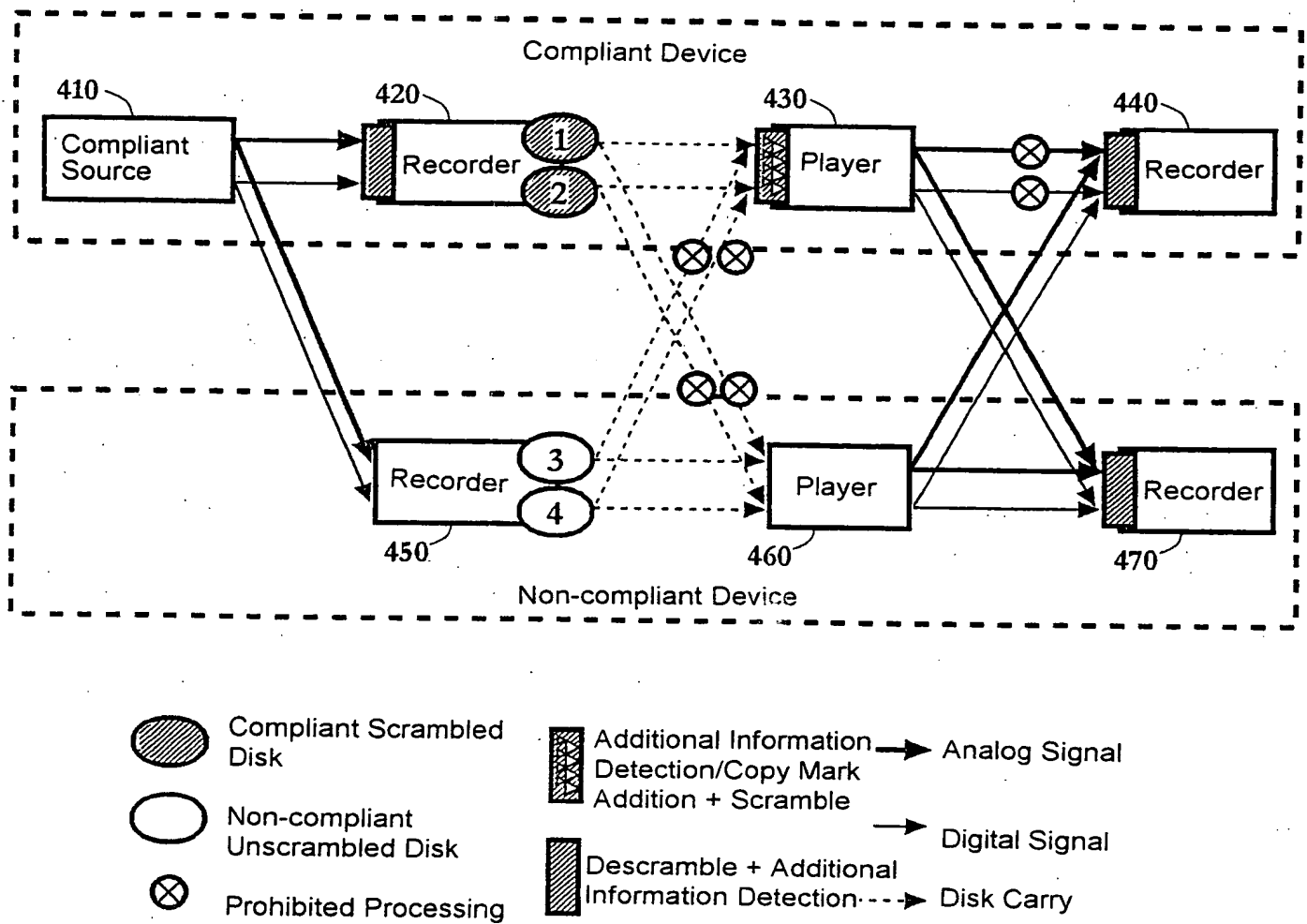
[Figure 2]



[Figure 3]

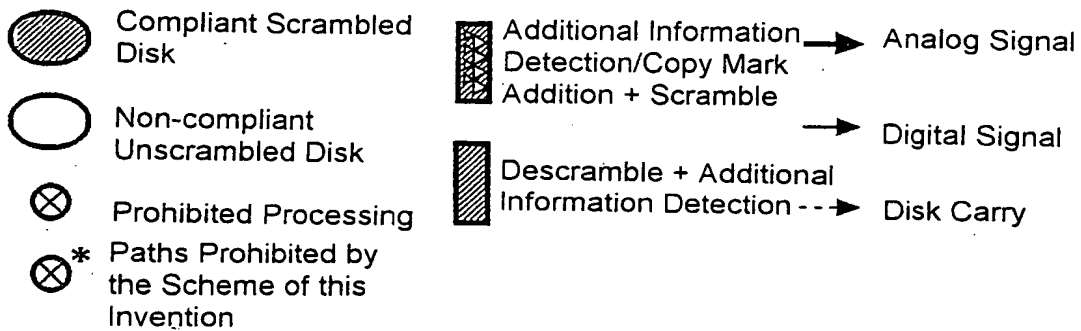
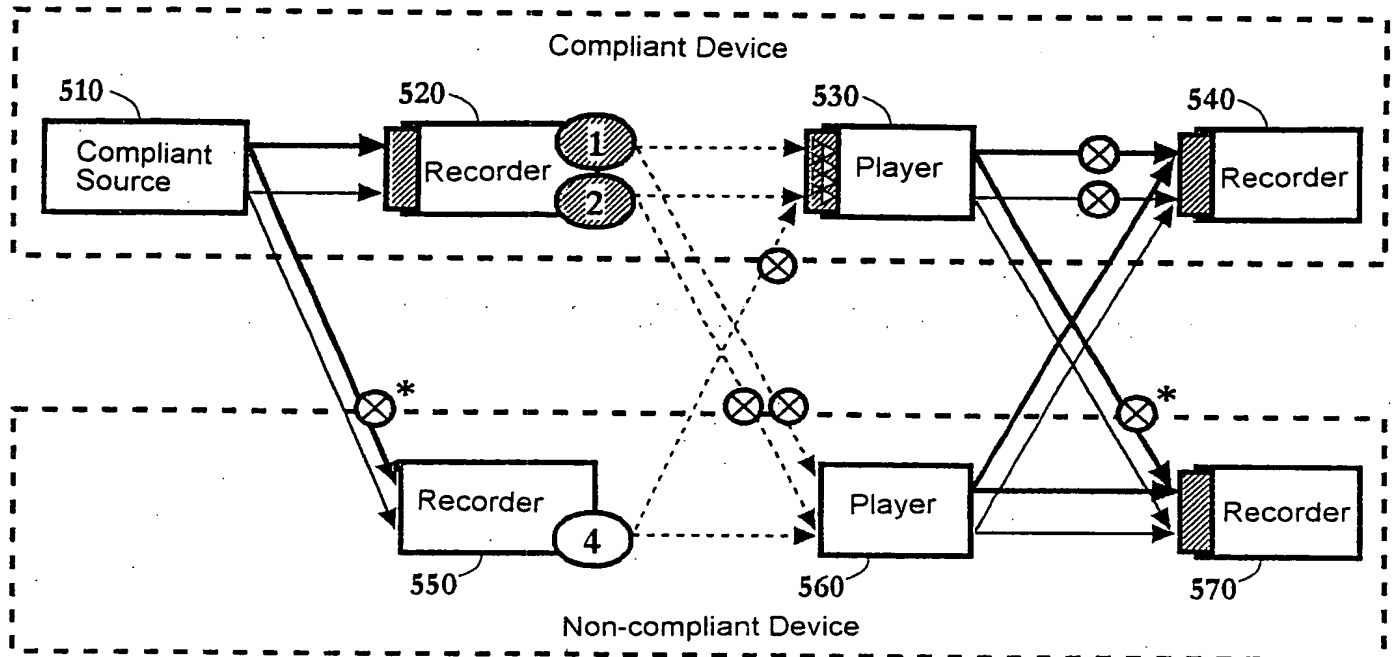


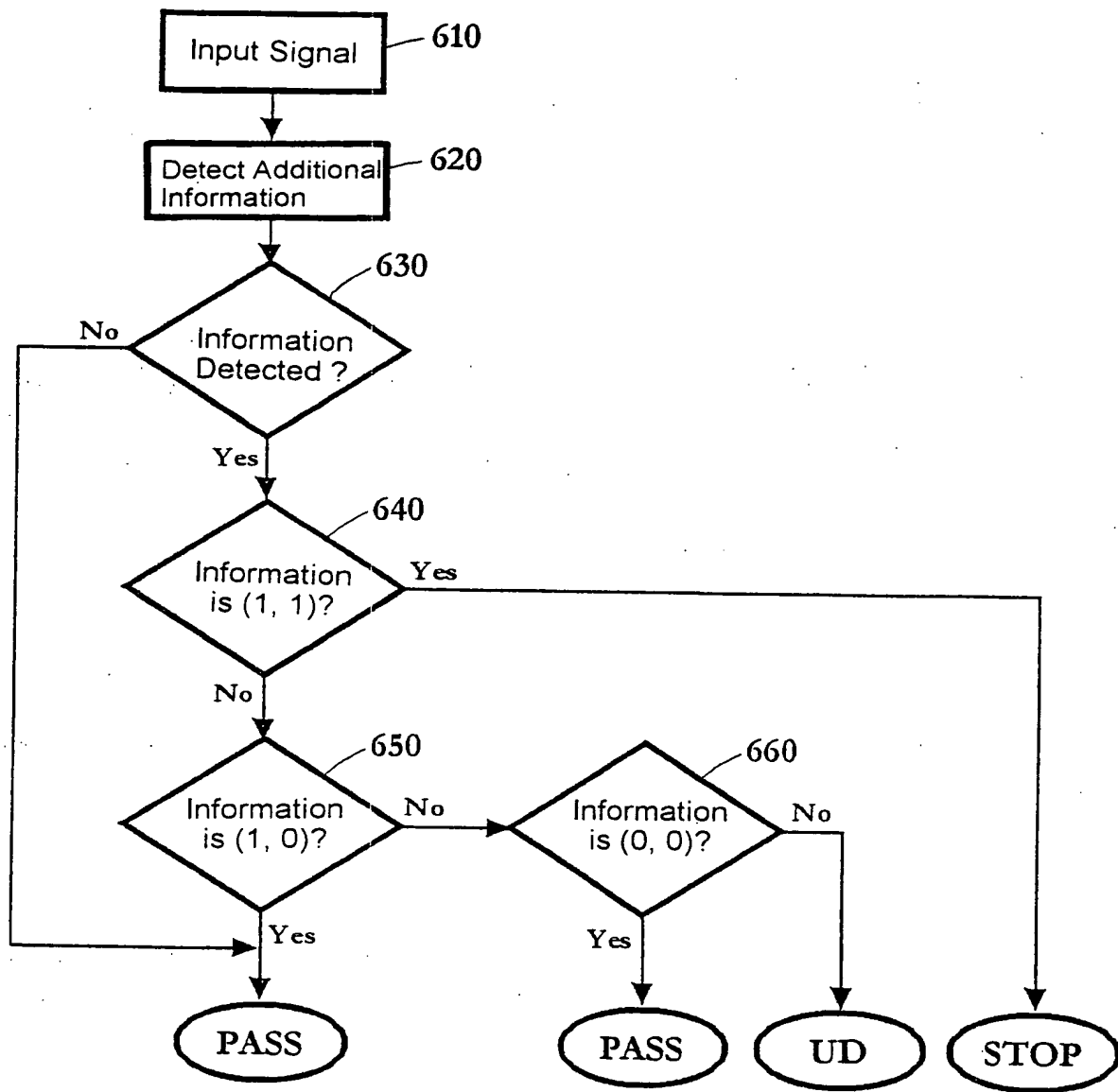
[Figure 4]





[Figure 5]



**PASS**

: Continue Copying Process

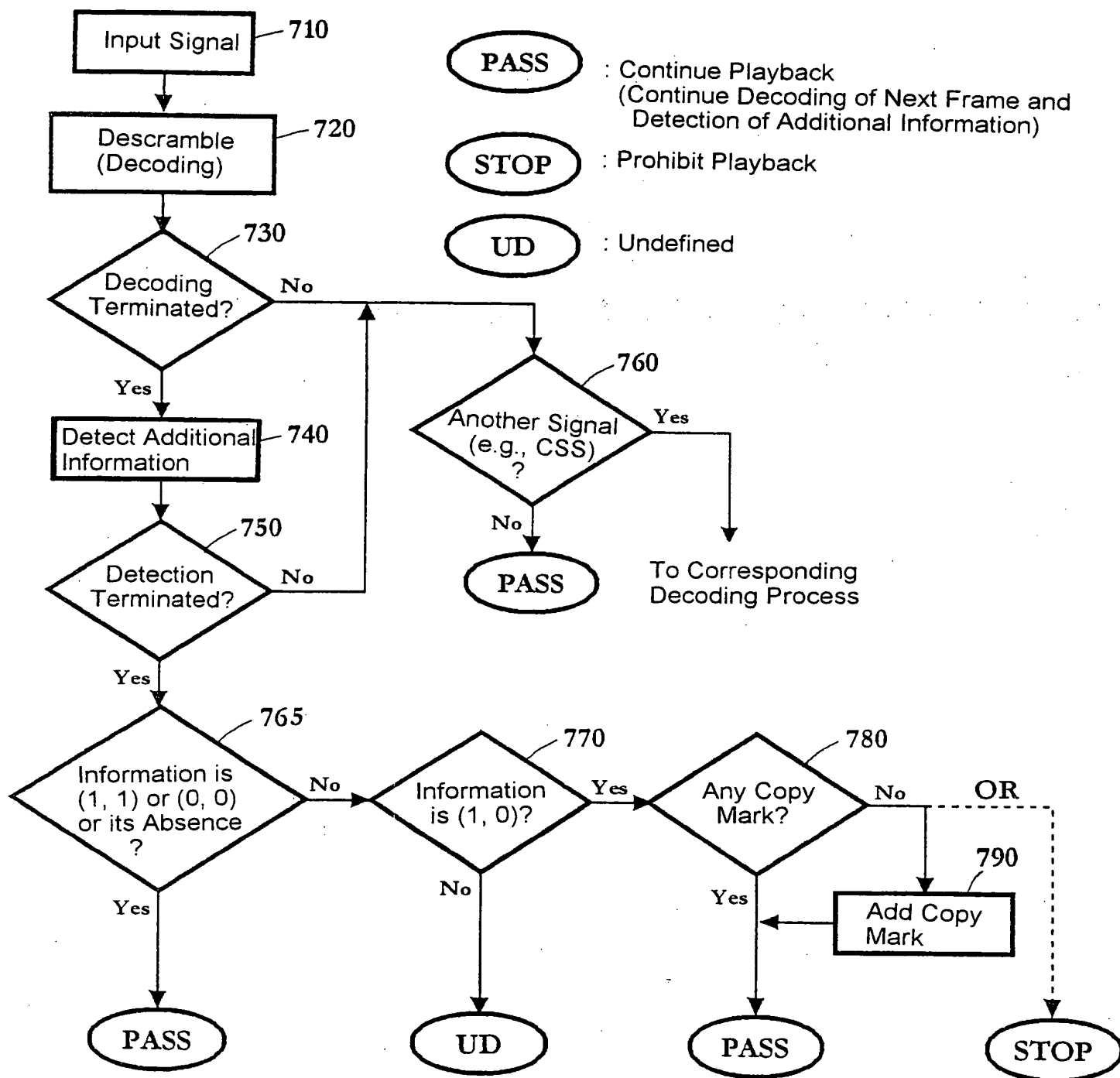
**STOP**

: Prohibit Copying Process

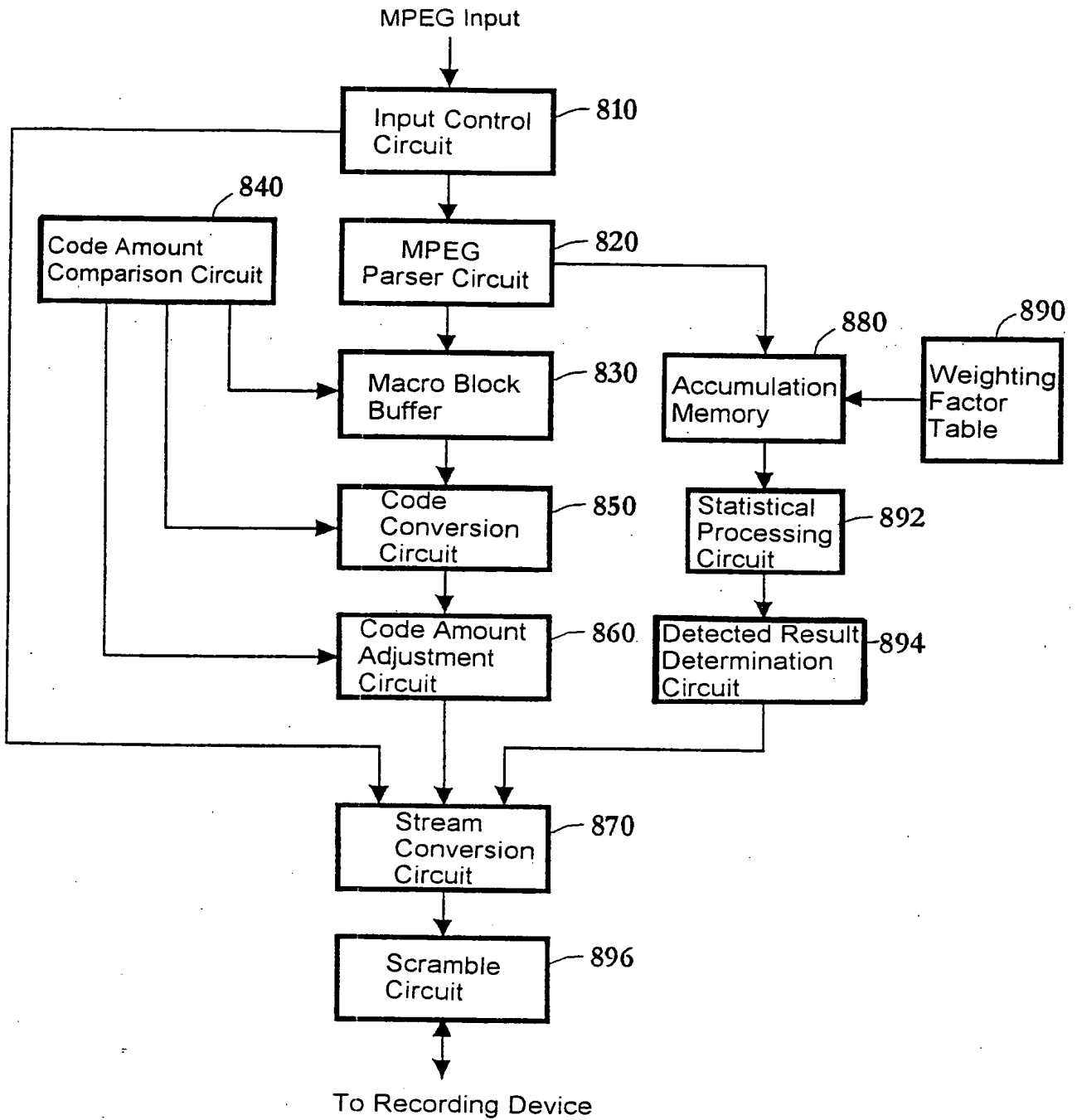
**UD**

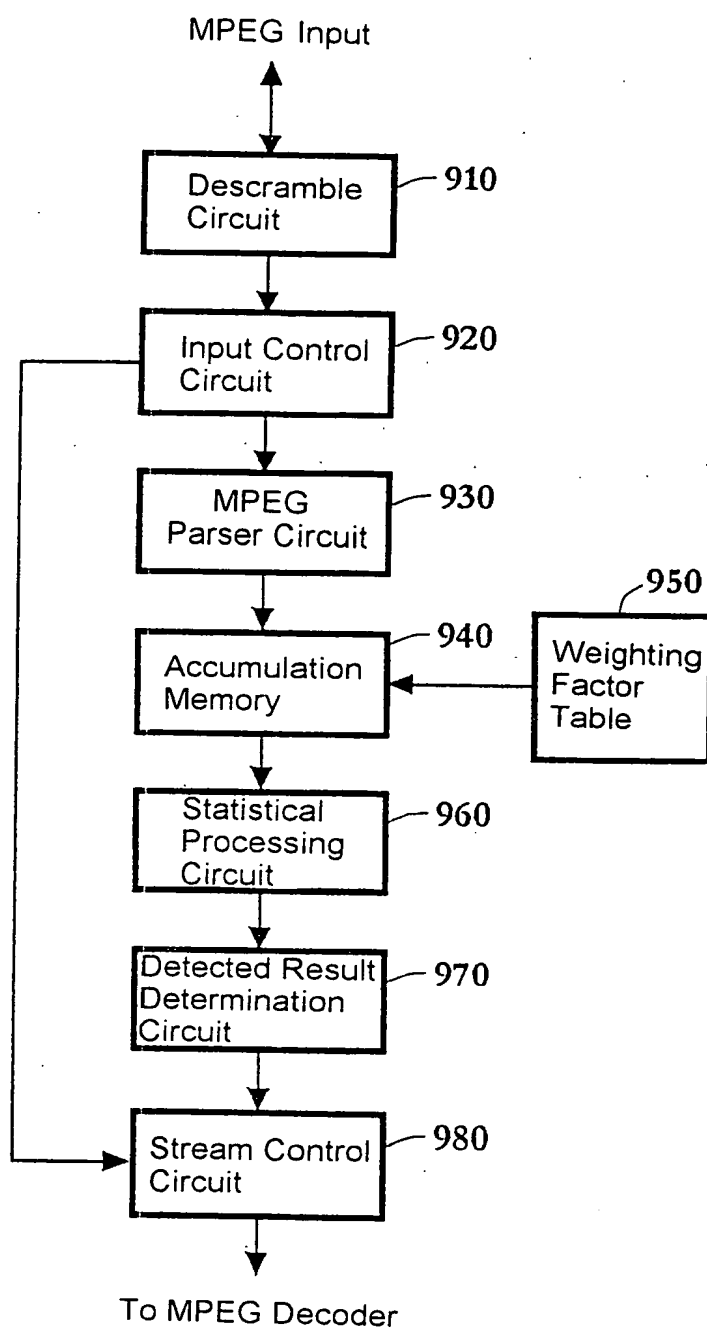
: Undefined

[Figure 7]



[Figure 8]





## 日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1998年11月13日

出 願 番 号

Application Number:

平成10年特許願第324169号

出 願 人

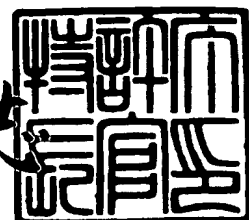
Applicant (s):

インターナショナル・ビジネス・マシーンズ・コーポレイション  
日本電気株式会社

1999年 6月 4日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建志



出証番号 出証特平11-3035975

【書類名】 特許願

【整理番号】 JA998171

【提出日】 平成10年11月13日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 01/00

【発明の名称】 デジタルデータ管理方法および装置

【請求項の数】 18

【発明者】

    【住所又は居所】 神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内

    【氏名】 三和 邦彦

【発明者】

    【住所又は居所】 神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内

    【氏名】 松芝 卓二

【発明者】

    【住所又は居所】 東京都府中市日新町1丁目10番 日本電気株式会社内

    【氏名】 田中 和佳

【特許出願人】

    【識別番号】 390009531

    【住所又は居所】 アメリカ合衆国10504、ニューヨーク州アーモンク  
        (番地なし)

    【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【特許出願人】

    【識別番号】 000004237

    【氏名又は名称】 日本電気株式会社

【代理人】

    【識別番号】 100065455

【弁理士】

【氏名又は名称】 山本 仁朗

【電話番号】 03-3366-6730

【手数料の表示】

【予納台帳番号】 050500

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 デジタルデータ管理方法および装置

【特許請求の範囲】

【請求項 1】

デジタルデータの媒体への記録方法であって、

- (1) デジタルデータから、電子的に埋め込まれた付加情報を検出する段階と、
  - (2) 付加情報が検出された場合、該付加情報を用いて、デジタルデータへのアクセス管理を行なう段階と、
  - (3) デジタルデータをスクランブルする段階と、
  - (4) 前記スクランブルされたデジタルデータを媒体へ記録する段階と、
- を有する、デジタルデータの記録方法。

【請求項 2】

前記アクセス管理を行なう段階 (2) が、デジタルデータの複製もしくは記録の停止、または、複製もしくは記録の続行を決定する段階である、請求項 1 記載の方法。

【請求項 3】

前記アクセス管理を行なう段階 (2) が、さらに前記付加情報の内容により、コピーマークをデジタルデータへ埋め込む段階を含む、請求項 2 記載の方法。

【請求項 4】

媒体に記録されたデジタルデータの再生管理を行なう方法であって、

- (1) スクランブルされたデジタルデータをデスクランブルする段階と、
  - (2) デジタルデータから、電子的に埋め込まれた付加情報およびコピーマークを検出する段階と、
  - (3) 前記付加情報とコピーマークを用いて、前記デジタルデータの再生管理を行なう段階と、
- を有する、デジタルデータの再生管理方法。

【請求項 5】

前記電子的に埋め込まれた付加情報が、データ自身の変形により埋め込まれた付加情報である、請求項 1 または請求項 4 の何れかに記載の方法。

【請求項 6】

デジタルデータを作成する、ビデオ・ドライバ・カードであって、

- (1) アナログデータを受け取り、デジタルデータを出力する、エンコーダと、
  - (2) 前記デジタルデータに電子的に埋め込まれた付加情報を検出する、付加情報検出手段と、
  - (3) 前記付加情報に従い、コピーマークを前記付加情報に付加する、コピーマーク付加手段と、
  - (4) デジタルデータ付加情報をスクランブルする手段と
- を有することを特徴とする、ビデオ・ドライバ・カード。

【請求項 7】

前記デジタルデータがMPEGストリームであり、前記エンコーダがMPEGエンコーダである、請求項 6 記載のビデオ・ドライバ・カード。

【請求項 8】

デジタルデータを復号する、ビデオ・ドライバ・カードであって、

- (1) スクランブルされたデジタルデータをデスクランブルする、デスクランブル手段と、
  - (2) デジタルデータから、電子的に埋め込まれた付加情報およびコピーマークを検出する、付加情報検出手段と、
  - (3) 前記付加情報とコピーマークを用いて、デジタルデータの再生管理を行なう手段と、
- を有することを特徴とする、ビデオ・ドライバ・カード。

【請求項 9】

前記デジタルデータがMPEGストリームであり、前記デジタルデータの再生管理が、MPEGストリームの出力を行なうか、行なわないかを決定し、所望のMPEGストリームを出力する手段である、請求項 8 記載のビデオ・ドライバ・カード。

【請求項 10】

前記電子的に埋め込まれた付加情報が、データ自身の変形により埋め込まれた付加情報である、請求項 6 または請求項 8 に記載のビデオ・ドライバ・カード。

【請求項 11】

前記デジタルデータの再生管理を行なう手段（3）が、さらに付加情報とコピーマークに従い、コピーマークをデジタルデータに付加して出力する手段を含む、請求項9記載のビデオ・ドライバ・カード。

【請求項 12】

デジタルデータを媒体に記録する、レコーダであって、

- （1）アナログデータを受け取り、デジタルデータを出力する、エンコーダと、
  - （2）前記デジタルデータに電子的に埋め込まれた付加情報を検出する、付加情報検出手段と、
  - （3）前記付加情報に従い、コピーマークを前記付加情報に付加する、コピーマーク付加手段と、
  - （4）デジタルデータをスクランブルする手段と、
  - （5）前記スクランブルされたデジタルデータを媒体に記録する手段と、
- を有することを特徴とする、レコーダ。

【請求項 13】

前記デジタルデータがMPEGストリームであり、前記エンコーダがMPEGエンコーダである、請求項12記載のレコーダ。

【請求項 14】

前記電子的に埋め込まれた付加情報が、データ自身の変形により埋め込まれた付加情報である、請求項12記載のレコーダ。

【請求項 15】

媒体に記録されたデジタルデータを再生する、プレイヤーであって、

- （1）媒体からデジタルデータを読み取る手段と、
  - （2）前記デジタルデータをデスクランブルする、デスクランブル手段と、
  - （3）デジタルデータから、電子的に埋め込まれた付加情報およびコピーマークを検出する、付加情報検出手段と、
  - （4）前記付加情報とコピーマークを用いて、デジタルデータの再生管理を行なう手段と、
- を有することを特徴とする、プレイヤー。

【請求項 16】

前記デジタルデータがMPEGストリームであり、前記デジタルデータの再生管理が、MPEGストリームの出力を行なうか、行なわないかを決定し、所望のMPEGストリームを出力する手段である、請求項 15 記載のプレイヤー。

【請求項 17】

前記電子的に埋め込まれた付加情報が、データ自身の変形により埋め込まれた付加情報である、請求項 15 記載のプレイヤー。

【請求項 18】

前記デジタルデータの再生管理を行なう手段（4）が、さらに付加情報とコピーマークに従い、コピーマークをデジタルデータに付加して出力する手段を含む、請求項 16 記載のプレイヤー。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタルコンテンツの著作権保護を行なう技術に関し、情報を電子透かしでデジタルコンテンツに埋め込み、これを録画機、再生機などで検出することによって、録画、再生を管理する方法および装置に関する発明である。より具体的には電子透かし技術と、スクランブル技術（あるいはエンクリプション）を用いた、録画、再生を管理する方法および装置に関する発明である。

【0002】

【従来の技術】

デジタルデータの著作権保護において、最も安全でかつ強力な管理機能を提供する方法の1つとして、電子透かしを用いたデータのアクセス管理手法がある。電子透かしとは、デジタルデータ（コンテンツ）に対して付加情報を電子的に埋め込む手法である。埋め込まれる付加情報は、データ自身の変形により埋め込まれる。つまりデジタルデータ（コンテンツ）と付加情報は一体となっており分離することは困難である。この電子透かしを用いてデータへのアクセス管理を行なう従来技術として、特願平 8-273551 号がある。特願平 8-273551 号では、付加情報検出器（電子透かし検出器）をDVDなどのドライブ内に設置

し、さまざまなMPEGストリームから検出し、これを用いてアクセス管理を行なう。図1にその概要図を示す。STB（セットトップボックス）から録画機120への信号としてはアナログまたはデジタルの場合がある。STBからMPEGストリームを流す場合は、録画機120内の付加情報検出器へ直接送られる。STBの出力がアナログの場合はビデオドライバカード内のMPEGエンコーダを経てデジタル信号を付加情報検出器に送る。付加情報検出器は、コンテンツに埋め込まれた付加情報およびコピーマーク情報を検出して、該情報に応じて、録画機120、再生機130に対して、予め定義された様々な管理を行なう。たとえば以下のような管理を行なう。

【0003】

・レコーディングデバイスにおいて電子透かしの検出を行い、それに基づいて、以下のコピー管理動作を行う。（なおCMはコピーマークの略である）

(1,0)かつCMなし：CMを追加してストリームを通す。（録画を許可する）

(1,0)かつCMあり：ストリーム、あるいは録画を停止する。

(1,1) : ストリーム、あるいは録画を停止する。

(0,0) or 付加情報検出なし：録画を許可する。

【0004】

・再生デバイスで電子透かしの検出を行い、それに基づいて、以下の再生管理動作を行う。

(1,0)かつCMなし：再生禁止。

(1,0)かつCMあり：再生専用ディスクからの読み出しなら再生禁止する。追記型、書き換え可能 ディスクからの読み出しなら再生許可する。

(1,1) : 再生専用ディスクからの読み出しなら再生許可する。追記型、書き換え可能 ディスクからの読み出しなら再生禁止する。

(0,0) or 付加情報検出なし：再生許可する。

【0005】

このように、特願平8-273551号はいくつかの複製管理、および媒体の種類に応じた再生管理技術を提供している。しかしながら、このような方法では、再生管理のため、付加情報検出器はドライブ内（レコーディングデバイス内、再

生デバイス内)に置く必要がある。なぜなら著作権保護を確実なものとするため、コスト的・スペース的に制約の厳しい録画機120の読み取り中核部に付加情報検出器を設置する必要があるからである。また電子透かし検出は、様々な種類のMPEGストリームから行う必要があり、検出器の規模が大きくなる。さらに再生機130において、コンテンツがコピーされたものであることを知るためには、読み出された媒体の種類情報(例えば再生専用、追記型、書き換え型)を知る必要がある。従って、このような問題のない電子透かしを用いた新しい著作権保護方式が望まれる。

## 【0006】

## 【発明が解決しようとする課題】

従って、本発明が解決しようとする課題は、コスト的・スペース的に制約の厳しいドライブ内に付加情報検出器を設置する必要のない、データの複製または再生管理方法、その装置を提供することである。

また別の課題は、付加情報検出のための検出器の規模が小さい、データの複製または再生管理方法、その装置を提供することである。

また別の課題は、再生管理において、媒体種類情報を知る必要のない、データの再生管理方法、その装置を提供することである。

また別の課題は、電子透かし技術とスクランブル技術を効果的に組み合わせた、データの複製または再生管理方法、そのシステムを提供することである。

## 【0007】

## 【課題を解決するための手段】

上記課題を解決するために、まず記録管理にあたっては、デジタルデータから、電子的に埋め込まれた付加情報を検出し、付加情報が検出された場合、該付加情報を用いて、デジタルデータへのアクセス管理を行なう。そしてデジタルデータをスクランブルし、スクランブルされたデジタルデータを媒体へ記録するように構成する。なお電子的に埋め込まれた付加情報とは、データ自身の変形により埋め込まれた付加情報を意味する。また、アクセス管理とは、デジタルデータの複製もしくは記録の停止、または、複製もしくは記録の続行を決定することを意味し、付加情報の内容によっては、コピーマークなどの管理情報をデジタルデー

タへ埋め込むことも行なう。

次に再生管理にあたっては、スクランブルされたデジタルデータをデスクランブルし、デスクランブルされたデジタルデータから、電子的に埋め込まれた付加情報およびコピーマークを検出する。そしてこれらの情報を用いて、デジタルデータの再生管理を行なうように構成する。

【0008】

図6に記録／複写管理のフローチャート例を示す。ステップ610でMPEGストリームなどのデジタルデータを入力し、ステップ620で電子的に埋め込まれた付加情報の検出を行なう、ステップ630で付加情報が検出されたかどうか判断し、検出されなければストリームはそのまま通過する。もしそのステップ630の判断がYESなら付加情報が(1, 1)かどうか判断し、そうであればストリームを通過させず、スクランブルあるいは録画を停止する。もし(1, 1)でなければステップ650で付加情報が(1, 0)かどうかを判断する。その結果がYESであればストリームは通過する。もしステップ650の結果がNOであれば、ステップ660で付加情報が(0, 0)かどうかを判断する。その結果がYESであればストリームは通過する。そうでなければ付加情報が(0, 1)の場合であり、本来このような付加情報はありえないので未定義と判断される。しかしながら媒体内でのビット化け、または埋め込み時の異常と考え、ストリームを禁止してもよい。通過したストリームはその後スクランブルして媒体に記録される。上記スクランブルは暗号化の一手段であるが、より強固にするために暗号キーに基づくスクランブルにしてもよい。この暗号キーによるスクランブルでは暗号キーが不明であればスクランブルを復号できないのでさらに安全なコンテンツの配布が可能となる。

【0009】

図7に再生管理のフローチャート例を示す。ステップ710でデジタルデータを入力し、ステップ720でスクランブルされたデジタルデータをデスクランブル(復号)する。ステップ730で復号が終了したかどうか判断し、終了していればステップ740へ処理は進む。もしステップ730の結果がNOであれば処理はステップ760で進みCSS(Content Scramble System)のような他の暗

号化手法がなされたものかどうか判断する。なおCSSとは再生専用ディスク用スクランブル手法である。もしステップ760の結果がYESであれば対応する復号処理を行なう。そうでなければ再生を継続する。ステップ740で付加情報の検出を行なった後、ステップ750で検出が終了したかどうかを判断する。その結果がNOであれば処理はステップ760へ進む。もしステップ750の結果がYESであれば処理はステップ765へ移る。ステップ765では検出した付加情報が(1, 1)または(0, 0)または付加情報がないか判断する。その結果がYESであれば再生は継続し、その結果がNOであればステップ770で付加情報が(1, 0)か判断する。もしその結果がNOであれば未定義となり、YESであればステップ780の判断に移る。ステップ780ではコピーマークがあるかどうか判断し、もしあれば再生を継続し、NOであればステップ790でコピーマークを付加して再生を継続する。ステップ780でコピーマークなしの場合には、再生をストップするようにしても構わない。

#### 【0010】

なお正しくデスクランブルされなかった場合（スクランブルされていない場合）の処理としては、以下のようにしてもよい。たとえば付加情報(1, 0)でかつコピーマークなしの場合、ストリームを停止し、デスクランブルあるいは再生を停止する。付加情報(1, 1)でかつコピーマークありの場合、ストリームを停止し、デスクランブルあるいは再生を停止する。付加情報(1, 1)の場合ストリーム、デスクランブルあるいは再生を停止する。付加情報(0, 0)または付加情報がない場合、再生を許可する。

#### 【0011】

#### 【発明の実施の形態】

以下、図面を参照して本発明の実施例を説明する。図2および図3には、本発明におけるデジタルデータの記録または再生を行なう装置の概観図が示されている。図2と図3の違いは、図2が主にパーソナルコンピュータなどにおいて用いられるビデオ・ドライバ・カードに本発明を適用した場合で、カードとドライバが区切られているの対して、図3は家電に代表されるデジタルレコーダおよびデジタルプレイヤーに本発明を適用した場合で、カードとドライブが一体となって



いる点が相違する。

【0012】

図2において、STB210に入力された信号が、STB210のアナログ出力から記録機220のビデオ・ドライバ・カードに入力される場合と、STB210内において、付加情報の検出、コピーマークの付加およびスクランブルを行ない、スクランブルされたデジタルデータを直接、記録機220のドライブに入力する場合がある。ビデオ・ドライバ・カードにアナログ信号が入力されると、MPEGエンコーダによりデジタルデータに変換され、付加情報の検出、コピーマークの付加が行われ、スクランブルされる。スクランブルされたデジタルデータはレコーディングデバイスにより媒体に記録される。媒体は再生機230に運ばれ再生される。ここで記録機220と再生機230は異なる装置として記載されているが、記録再生を同一の装置として構成してもよい。またそのほうがより一般的であろう。再生機230に運ばれた媒体は、再生デバイスによりデジタルデータが読み取られる。読み取られたデジタルデータはビデオ・ドライバ・カードに入力され、デスクランブル、および付加情報検出、必要に応じてコピーマークの付加が行われる。そしてMPEGデコーダにより復号される。

【0013】

図3において、STB310に入力された信号が、STB310のアナログ出力からレコーダ320に入力される場合と、STB310内において、付加情報の検出、コピーマークの付加およびスクランブルを行ない、スクランブルされたデジタルデータを直接、レコーダ320のドライブに入力する場合がある。レコーダにアナログ信号が入力されると、MPEGエンコーダによりデジタルデータに変換され、付加情報の検出、コピーマークの付加が行われ、スクランブルされる。スクランブルされたデジタルデータはレコーディングデバイスにより媒体に記録される。媒体はプレイヤー330に運ばれ再生される。ここでレコーダ320とプレイヤー330は異なる装置として記載されているが、記録再生を同一の装置として構成してもよい。またそのほうがより一般的であろう。プレイヤー330に運ばれた媒体は、デジタルデータが読み取られる。読み取られたデジタルデータはデスクランブル、および付加情報およびコピーマークの検出が行われ、

必要に応じてコピーマークがデジタルデータに付加されて出力される。そしてMPEGデコーダによりアナログ信号に変換される。

#### 【0014】

レコーダ320もしくはSTB内における電子透かしおよびスクランブルのより詳細な装置構成ブロック図を図8に示す。ブロック810は、MPEGデータを受け取り、MPEGストリームをストリーム変換回路およびMPEGパーサー回路に渡す入力制御回路ブロックである。ブロック820は、MPEGストリームより次の段に必要な部分を抽出する、MPEGパーサー回路ブロックである。ブロック830は、管理情報埋め込みに必要なマクロブロックを格納する、マクロブロックバッファである。ブロック840はマクロブロック中の符号長を計算比較する、符号量比較回路ブロックである。ブロック850は符号を管理情報を埋め込むために変換する、符号変換回路ブロックである。ブロック860は符号長が変換前と変わらないように調整し、結果を埋め込み変換テーブルとしてまとめる、符号量調整回路ブロックである。ブロック870は付加情報検出結果に基づいて、MPEGストリームを止めたり、変換したり、そのまま通過させる、ストリーム変換回路ブロックである。ブロック880はMPEGパーサー回路より取り出されたDCT係数と重み付け係数とを掛け算した値を累積する累積メモリ回路ブロックである。ブロック890は入力MPEG画像に含まれる、付加情報と相関をとるための重み付け係数テーブルである。ブロック892は累積メモリに貯えられた値を統計処理する、統計処理回路ブロックである。ブロック897は埋め込まれた付加情報の値を前段より判定しストリーム変換回路に指示を出す、検出結果判定回路ブロックである。ブロック896はレコーディングデバイスと認証(Authentication)を行い、付加情報が検出されたストリームに対して、スクランブルをかける、スクランブル回路ブロックである。

#### 【0015】

プレイヤー330におけるデスクランブルと付加情報の検出のより詳細な装置構成ブロック図を図9に示す。ブロック910は入力されたデジタルデータを、プレーイングデバイス(Playing Device)と認証を行い、スクランブルを解除する、デスクランブル回路ブロックである。ブロック920は、デスクランブル回路

からMPEG ストリームを受け取りストリーム制御回路および MPEG パーサー回路に渡す、入力制御回路ブロックである。ブロック 930 は、MPEG ストリームより次の段に必要な部分を抽出する、MPEG パーサー回路ブロックである。ブロック 940 はMPEG パーサー回路より取り出されたDCT係数と重み付け係数とを掛け算した値を累積する累積メモリー回路ブロックである。ブロック 950 は入力MPEG 画像に含まれる、付加情報と相関をとるための重み付け係数テーブルである。ブロック 960 は、累積メモリーに貯えられた値を統計処理する、統計処理回路ブロックである。ブロック 970 は埋め込まれた付加情報の値を前段より判定しストリーム制御回路に指示を出す、検出結果判定回路ブロックである。ブロック 980 は、付加情報検出結果に基づいて、MPEG ストリームを止めたり、そのまま通過させる、ストリーム制御回路である。

## 【0016】

図4に従来の方法により、操作が禁止される信号および媒体のパスを示す。コンプライアント・デバイス（従来の方式に従ったデバイス）内では、コンプライアントソース（従来の方式に従ったソース）410がレコーダ420、プレイヤー430において操作がスムーズに行われる。しかしさらなる記録をレコーダ440にて行なうことはできない。しかしながら、ノン・コンプライアント・デバイスと組み合わせた動作において、違法な記録再生が可能となる。たとえばコンプライアントソース410がノン・コンプライアント・デバイス内のレコーダ450にデジタル入力された場合、そのデジタル記録が可能であること、またその再生がプレイヤー460において可能であることがその例である。その他、コンプライアント・デバイスのプレイヤー430のデジタル出力がノン・コンプライアント・デバイス内のレコーダ470に入力された場合その記録が可能となる。

## 【0017】

図5に本発明の方法により、操作が禁止される信号および媒体のパスを示す。コンプライアント・デバイス（本発明の方式に従ったデバイス）内では、コンプライアントソース（本発明の方式に従ったソース）510がレコーダ520、プレイヤー530において操作がスムーズに行われる。しかしさらなる記録をレコーダ540にて行なうことはできない。ここでノン・コンプライアント・デバイ

スと組み合わせた動作を見る。まずコンプライアントソース 510 がノン・コンプライアント・デバイス内のレコーダ 550 にデジタル入力をしようとしても禁止されるのでデジタル記録は不可能である。したがってプレイヤー 560 においてデジタル再生は不可能となる。またコンプライアント・デバイスのプレイヤー 530 のデジタル出力がノン・コンプライアント・デバイス内のレコーダ 570 に入力されることも禁止できる。

## 【0018】

また再生管理における別の実施例として、CSS のような再生専用ディスク用スクランブルされたコンテンツに対しては、CSS が正しくデスクランブルされたことをもって、再生を可能としてもよい。たとえば CSS が正しくデスクランブルされたら電子透かしの検出を行わないようにし、CSS が正しくデスクランブルされたら付加情報(1,1)でも再生する。またデスクランブラを、直前で検出した電子透かし情報や、付加情報をキーなどとして用いて行う、あるいは初期デスクランブル後に検出した電子透かし情報を用いて、以降のデスクランブルを行う方式を追加することによって、スクランブルの保護機能強化、電子透かしの検出の義務づけを行うことも可能である。スクランブルされたままでのコピーに関しては、暗号キーによるスクランブル等で、コピーしても再生を不能とすることができる。その他、著作権保護の対象でないコンテンツは、スクランブル、付加情報の埋め込みをしないようにしてもよいし、デスクランブルをテレビ等の表示機内でのデスクランブル、付加情報の検出を行うように応用することも、本発明の本質を逸脱することなく同様に実施可能である。

## 【0019】

## 【発明の効果】

本発明により、電子透かし技術とスクランブル技術を効果的に組み合わせた、デジタルデータの複製または再生管理方法、その装置が提供される。これにより、コスト的・スペース的に制約の厳しいドライブ内に付加情報検出器を設置する必要がなくなる。さらに、コンプライアントソースのノン・コンプライアント・デバイス内のレコーダによるデジタル記録、およびプレイヤーによるデジタル再生を禁止することが可能となる。

【図面の簡単な説明】

【図 1】

データのアクセス管理を行なう従来技術を表す図である。

【図 2】

本発明におけるデジタルデータの記録または再生を行なう装置の概観図である。

【図 3】

本発明におけるデジタルデータの記録または再生を行なう装置の別の概観図である。

【図 4】

従来の方法により操作が禁止される信号および媒体のパスを示す図である。

【図 5】

本発明の方法により操作が禁止される信号および媒体のパスを示す図である。

【図 6】

記録／複写管理のフローチャート例である。

【図 7】

再生管理のフローチャート例である。

【図 8】

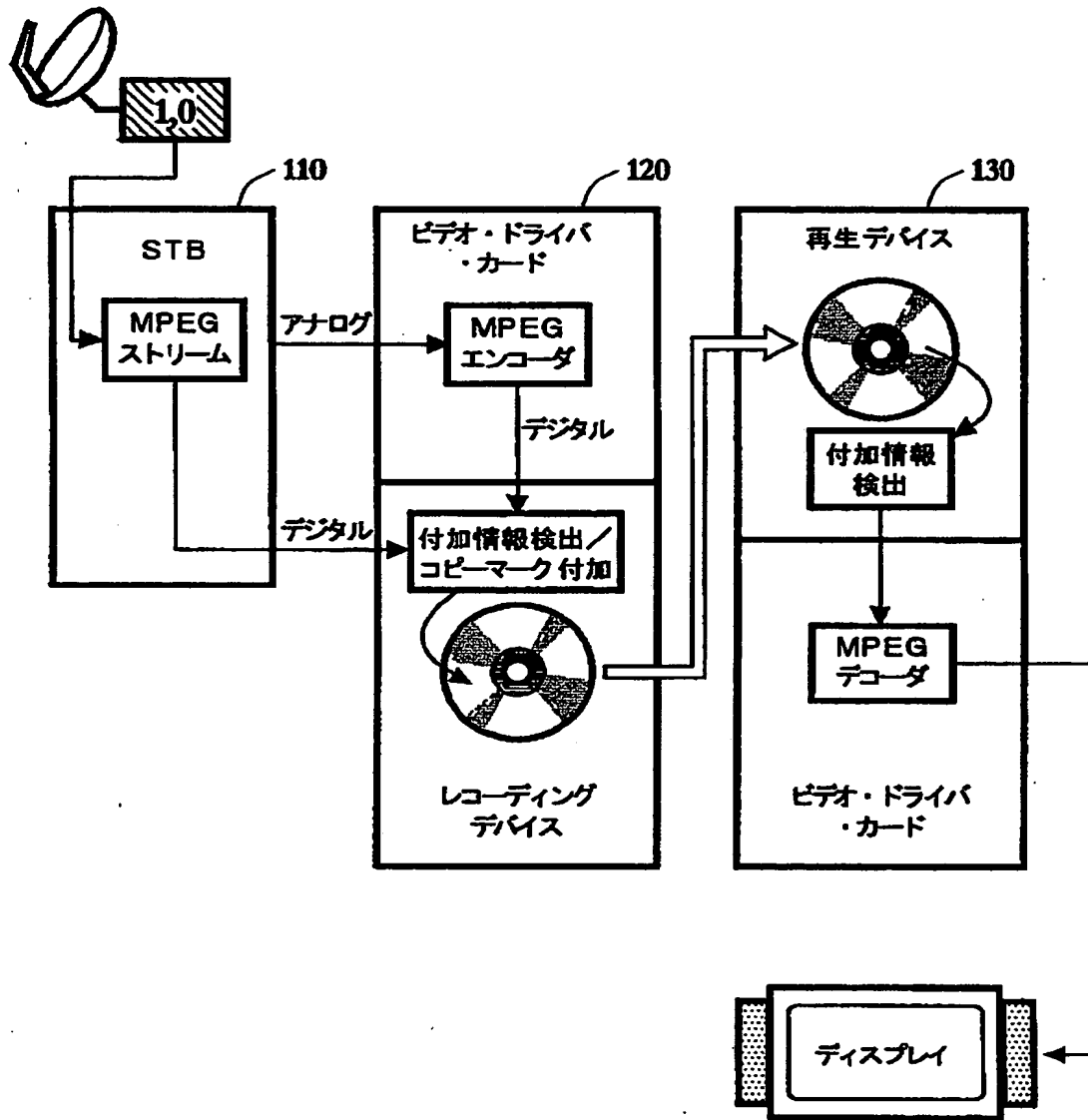
電子透かしおよびスクランブルのより詳細な装置構成例を示すブロック図である。

【図 9】

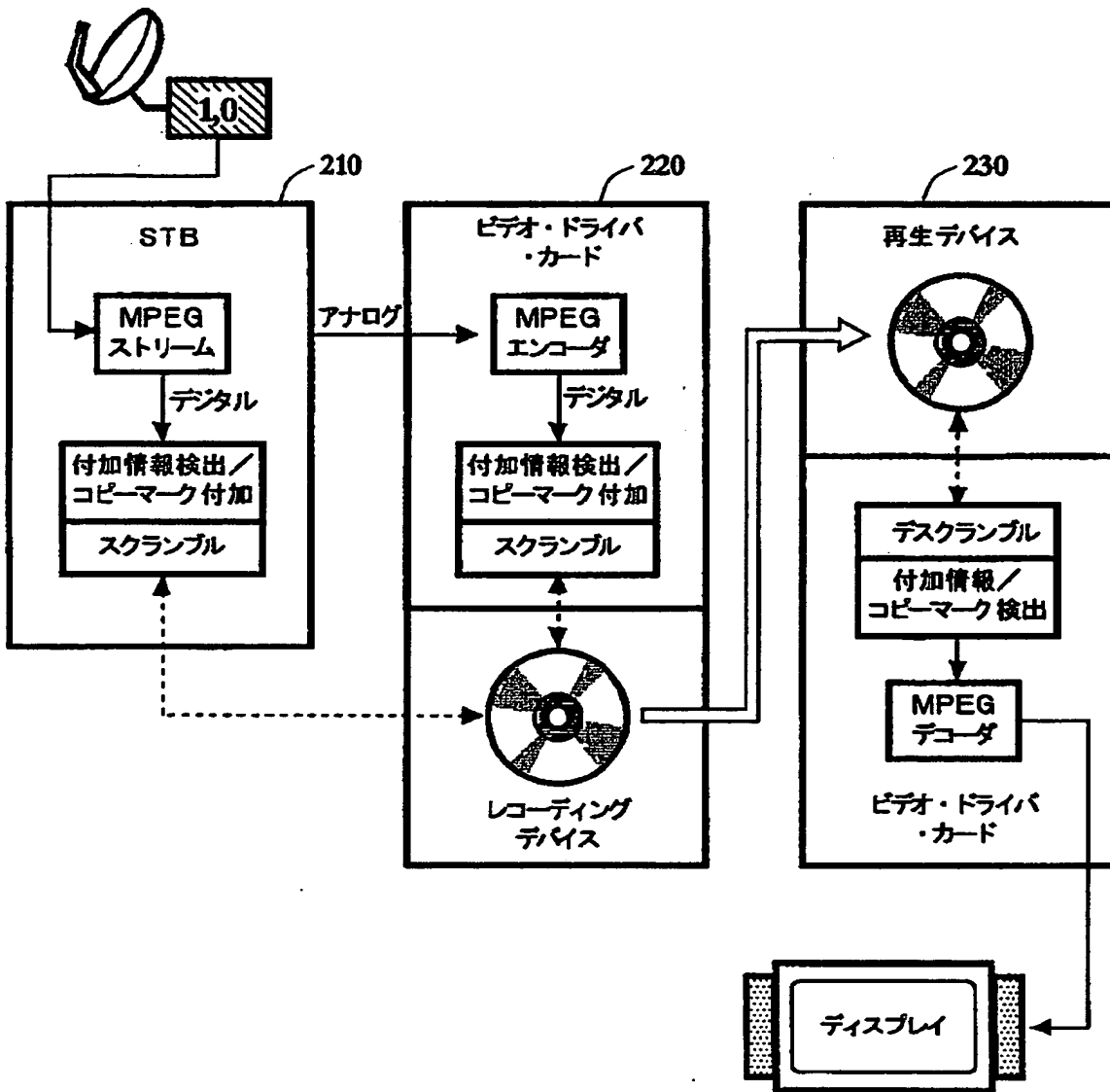
デスクランブルと付加情報の検出のより詳細な装置構成例を示すブロック図である。

【書類名】 図面

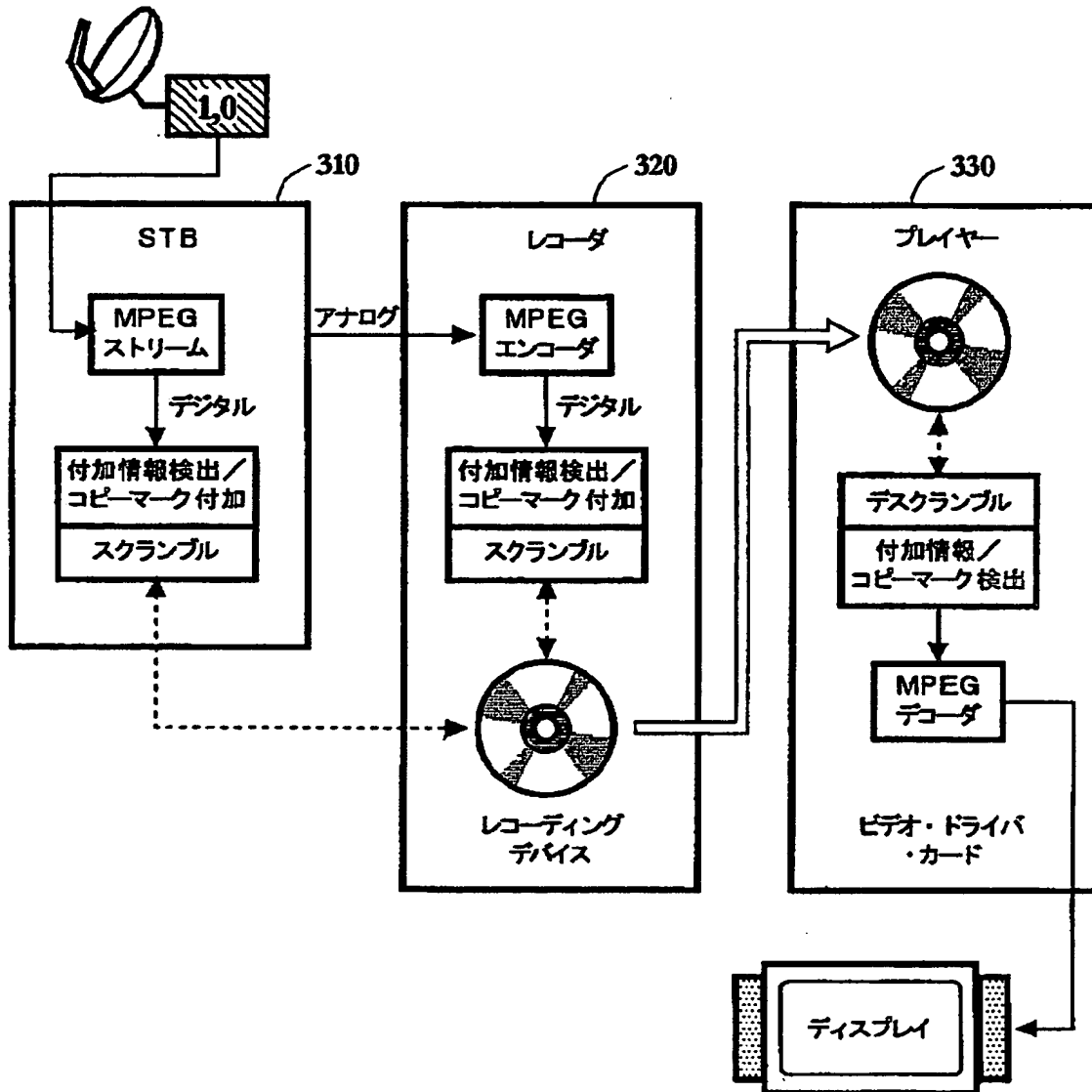
【図 1】



【図 2】

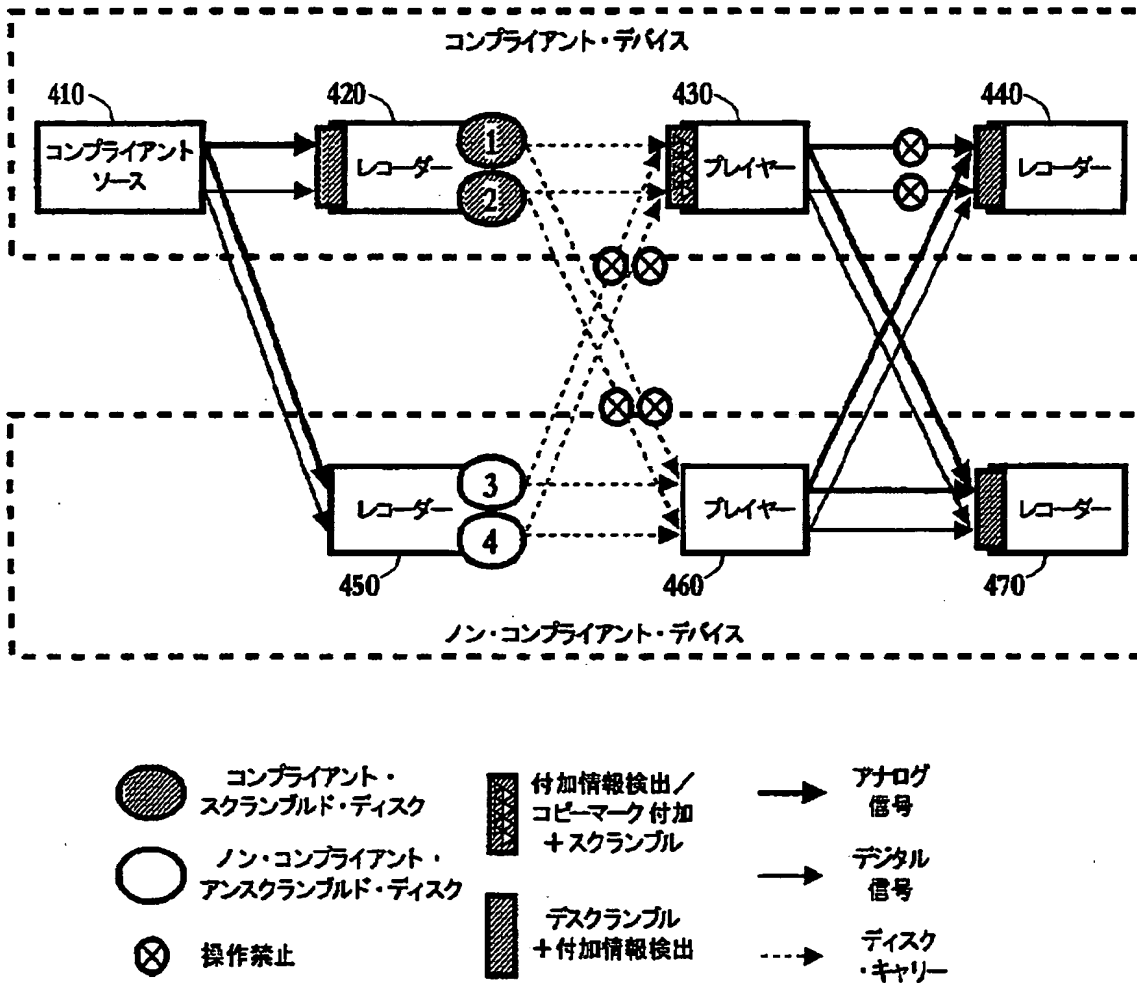


【図 3】

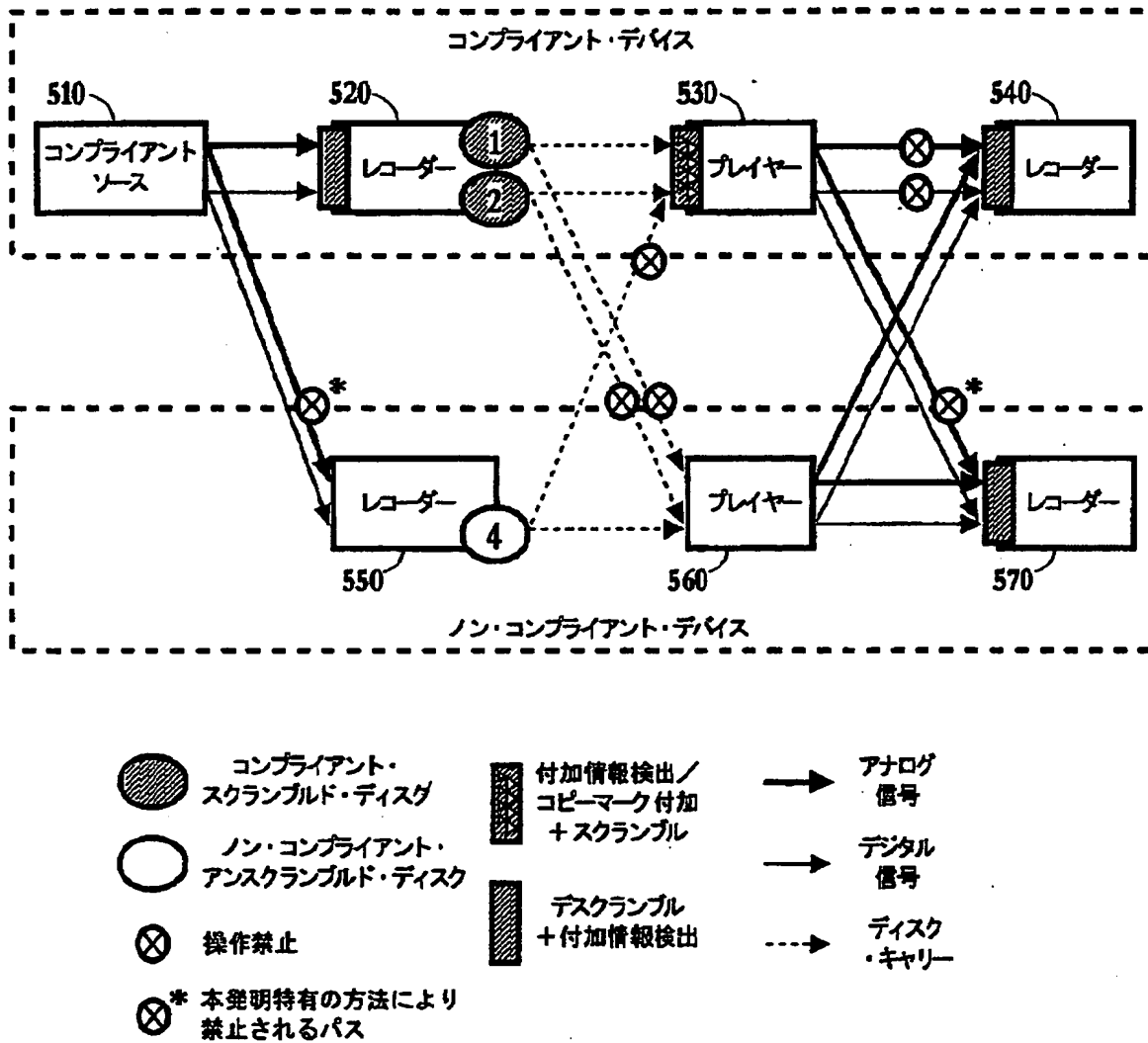




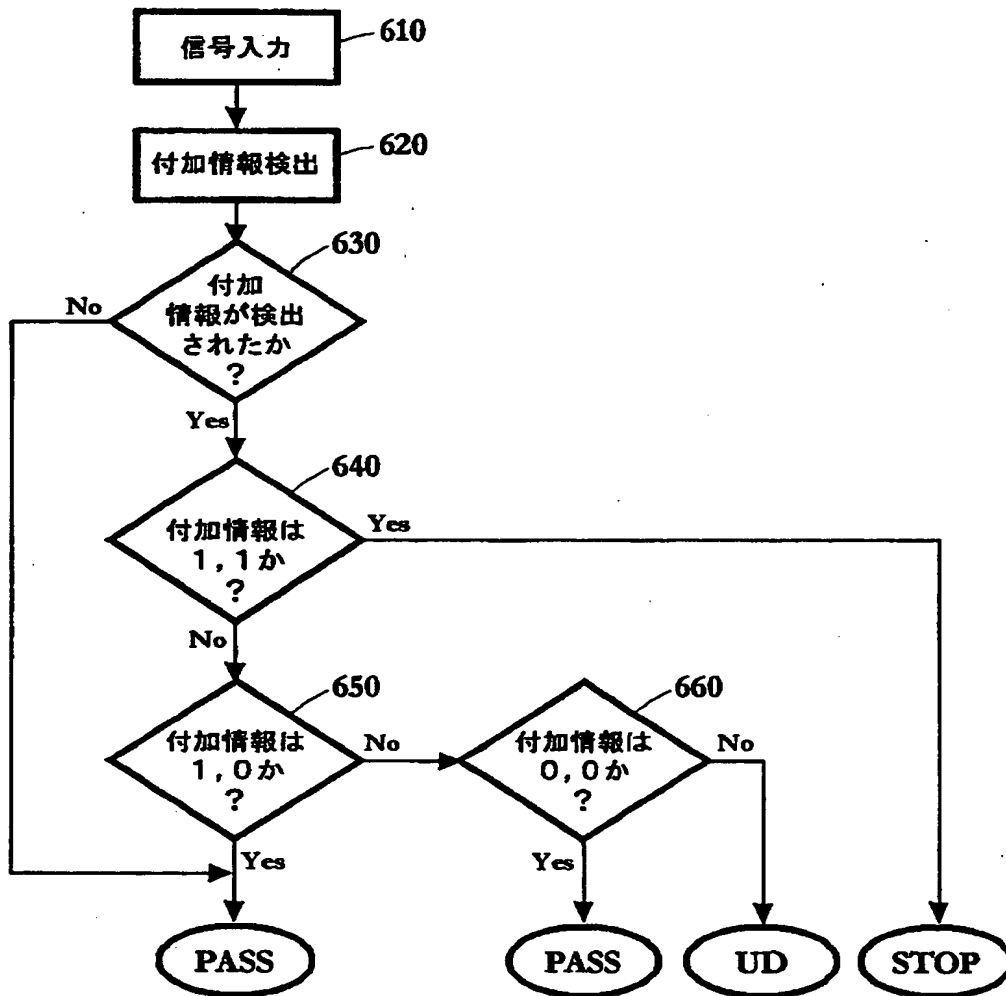
【図4】



【図 5】



【図 6】

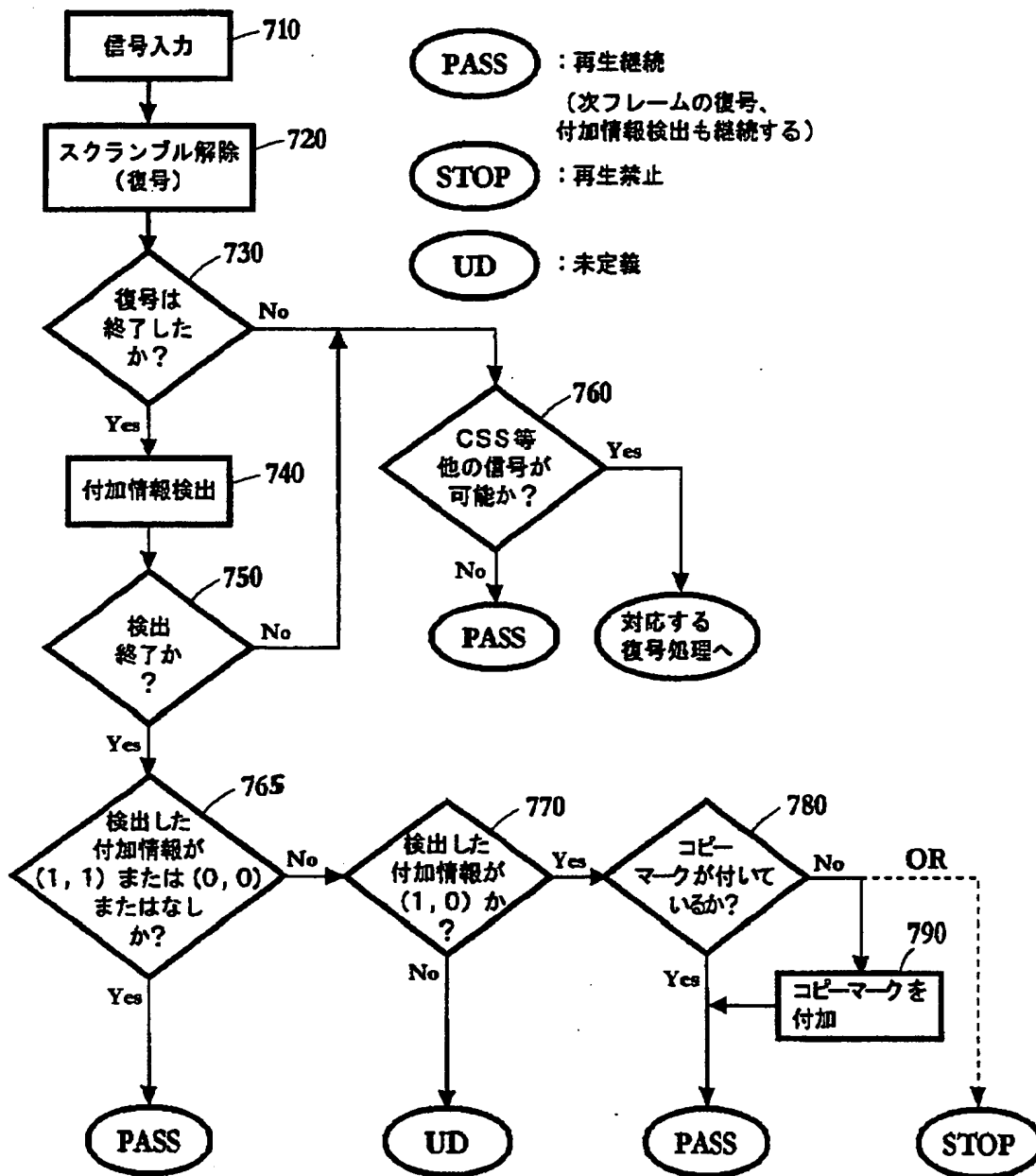


**PASS** : 複製処理の継続

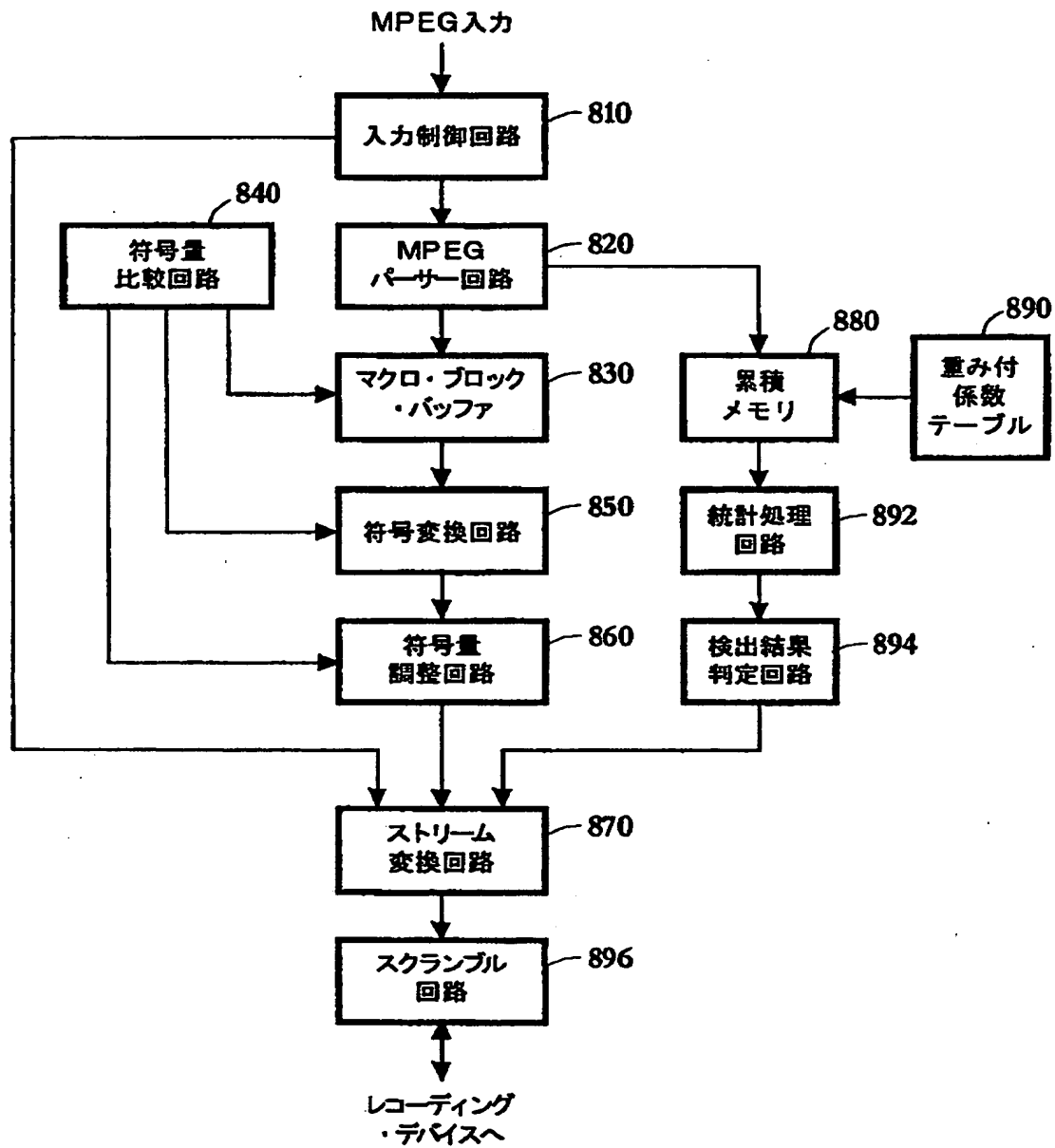
**STOP** : 複製処理の禁止

**UD** : 未定義

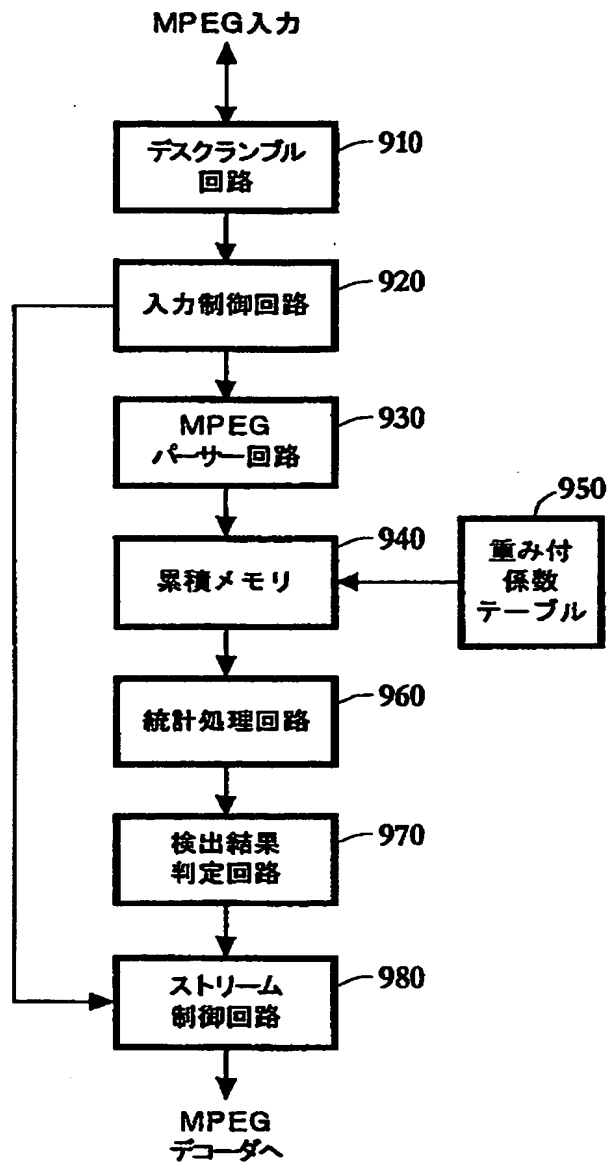
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】コスト的・スペース的に制約の厳しいドライブ内に付加情報検出器を設置する必要のない、データの複製または再生管理方法、その装置を提供することである。

【解決手段】まず記録管理にあたっては、デジタルデータから、電子的に埋め込まれた付加情報を検出し、付加情報が検出された場合、該付加情報を用いて、デジタルデータへのアクセス管理を行なう。そしてデジタルデータをスクランブルし、スクランブルされたデジタルデータを媒体へ記録するように構成する。なお電子的に埋め込まれた付加情報とは、データ自身の変形により埋め込まれた付加情報を意味する。また、アクセス管理とは、デジタルデータの複製もしくは記録の停止、または、複製もしくは記録の続行を決定することを意味し、付加情報の内容によっては、コピーマークなどの管理情報をデジタルデータへ埋め込むことも行なう。

次に再生管理にあたっては、スクランブルされたデジタルデータをデスクランブルし、デスクランブルされたデジタルデータから、電子的に埋め込まれた付加情報およびコピーマークを検出する。そしてこれらの情報を用いて、デジタルデータの再生管理を行なうように構成する。

【選択図】 図3

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】  
【識別番号】 390009531  
【住所又は居所】 アメリカ合衆国 10504、ニューヨーク州 アー  
モンク (番地なし)  
【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コー  
ポレーション

【特許出願人】  
【識別番号】 000004237  
【住所又は居所】 東京都港区芝五丁目 7 番 1 号  
【氏名又は名称】 日本電気株式会社

【代理人】 申請人  
【識別番号】 100065455  
【住所又は居所】 東京都新宿区西新宿七丁目 21 番 1 号 新宿ロイヤ  
ルビル 3 階 山本特許事務所  
【氏名又は名称】 山本 仁朗



出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 1990年10月24日

[変更理由] 新規登録

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレイション

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日  
[変更理由] 新規登録  
住 所 東京都港区芝五丁目7番1号  
氏 名 日本電気株式会社